

COMMUNICATIONS INSTRUCTIONS INTERNET PROTOCOL (IP) SERVICES

ACP 201



MARCH 2009

Uncontrolled Copy When Printed

FOREWORD

1. The Combined Communications-Electronics Board (CCEB) is comprised of the five member nations, Australia, Canada, New Zealand, United Kingdom and United States and is the Sponsoring Authority for all Allied Communications Publications (ACPs). ACPs are raised and issued under common agreement between the member nations.
2. ACP 201, COMMON INSTRUCTIONS ELECTRONIC INTERNET PROTOCOL (IP) SERVICES, is an UNCLASSIFIED CCEB publication.
3. This publication contains Allied military information for official purposes only.
4. It is permitted to copy or make extracts from this publication.
5. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP198.

THE COMBINED COMMUNICATION-ELECTRONICS BOARD
LETTER OF PROMULGATION
FOR ACP 201

1. The purpose of this Combined Communication Electronics Board (CCEB) Letter of Promulgation is to implement ACP 201 within the Armed Forces of the CCEB Nations. ACP 201 COMMUNICATION INSTRUCTIONS INTERNET PROTOCOL (IP) SERVICES, is an UNCLASSIFIED publication developed for Allied use and, under the direction of the CCEB Principals. It is promulgated for guidance, information, and use by the Armed Forces and other users of military communications facilities.
2. ACP 201 is effective on receipt for CCEB Nations and when determined by the NATO Military Committee (NAMILCOM) for NATO nations and Strategic Commands.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 201	CCEB	On Receipt	LOP

3. All proposed amendments to the publication are to be forwarded to the national coordinating authorities of the CCEB.

For the CCEB Principals

Paul Foster

P. FOSTER
Major, CF
CCEB Permanent Secretary

RECORD OF PAGE CHECKS

Date Checked	By Whom Checked (Signature & Rank)	Date Checked	By Whom Checked (Signature & Rank)

Uncontrolled Copy When Printed

RECORD OF MESSAGE CORRECTIONS

Identification of Message Correction and Date Time Group (DTG)		Date Entered	Entered by (Signature, Rank, Grade or Rate and Name of Command)
DTG	Correction		

Uncontrolled Copy When Printed

TABLE OF CONTENTS

FOREWORD	ii
LETTER OF PROMULGATION	iii
RECORD OF PAGE CHECKS	iv
RECORD OF MESSAGE CORRECTIONS	v
TABLE OF CONTENTS	vi
LIST OF FIGURES AND TABLES	viii
CHAPTER 1	1-1
GENERAL INSTRUCTIONS	1-1
OVERVIEW	1-1
BACKGROUND	1-1
PURPOSE	1-2
SCOPE	1-2
TACTICAL MESSAGING SYSTEMS	1-3
SECURITY	1-3
DEFINITIONS	1-3
MODUS OPERANDI	1-4
ELEMENTS OF SERVICE	1-6
FUNCTIONAL (ROLE BASED) ACCOUNTS	1-6
MANAGING NETWORK OVERHEADS	1-6
TRAINING	1-7
CHAPTER 2	2-8
E-MAIL	2-8
BACKGROUND	2-8
SHORTCOMINGS	2-8
RESPONSIBILITY	2-9
WHEN TO USE E-MAIL	2-9
E-MAIL FORMAT	2-9
PRECEDENCE MARKERS	2-10
ACKNOWLEDGEMENT REQUEST	2-11
ACKNOWLEDGEMENT REPLY	2-11
ACTION ADDRESSEES (TO)	2-12
INFORMATION ADDRESSEES (CC/BCC)	2-12
GLOBAL ADDRESS LISTS	2-12
ATTACHMENTS	2-12
WEBMAIL	2-13
ROLE BASED ACCOUNTS	2-13
EMAIL ETIQUETTE	2-13
ANNEX A TO CHAPTER 2	2A-1
ANNEX B TO CHAPTER 2	2B-1
ANNEX C TO CHAPTER 2	2C-1
CHAPTER 3	3-1
CHAT	3-1

UNCLASSIFIED

ACP 201

INTRODUCTION	3-1
OVERVIEW	3-1
CHAT MESSAGE FORMAT	3-3
TACTICAL USE OF CHAT	3-4
MEETING ROOMS	3-4
MEETING ROOM MODERATORS	3-5
MEETING ROOM WATCH REQUIREMENTS	3-5
MONITORING CHAT ROOMS	3-6
DIRECTED AND FREE NETS	3-6
THE EXECUTIVE METHOD	3-6
OPERATING RULES	3-7
BREVITY	3-7
AUTHENTICATION	3-8
ACKNOWLEDGMENT OF MESSAGES	3-8
VERIFICATION	3-9
GENERAL OPERATOR TECHNIQUES	3-9
CHAT APPLICATIONS	3-11
LOTUS SAMETIME	3-11
PERSISTENT CHAT	3-12
ANNEX A TO CHAPTER 3	3A-1
ANNEX B TO CHAPTER 3	3B-1
ANNEX C TO CHAPTER 3	3C-1
CHAPTER 4	4-1
WEB SERVICES	4-1
INTRODUCTION	4-1
COLLABORATION	4-1
COLLABORATION AT SEA (CAS)	4-2
WEB POLICY	4-3
ANNEX A TO CHAPTER 4	4A-1

Uncontrolled Copy When Printed

LIST OF FIGURES AND TABLES

Figure 1 – CENTRIXS Hub Page	2B-2
Figure 2 - CAS Login Screen.....	2B-2
Figure 3 – Webmail Link	2B-3
Figure 4 - Mail Tab	2B-3
Figure 5 - Example of Long Chat Message	3-9
Figure 6 - Sametime Connect	3B-1
Figure 7 - Login Screen	3B-2
Figure 8 - Activity Status	3B-2
Figure 9 - Logging Off Sametime Connect	3B-3
Figure 10 - Adding Users to Personal Groups	3B-4
Figure 11 - Add Person or Group	3B-5
Figure 12 - Directory Listing	3B-6
Figure 13 - Selecting/Adding Users.....	3B-7
Figure 14 - Personal Buddy List	3B-7
Figure 15 - Adding User Groups	3B-8
Figure 16 - Selecting/Adding User/Staff Groups.....	3B-9
Figure 17 - Group Contents	3B-9
Figure 18 - Staff Groups in Buddy List	3B-10
Figure 19 - Creating an Impromptu Meeting Room	3B-11
Figure 20 - Message Box	3B-11
Figure 21 - Chat Window	3B-12
Figure 22 - Invite additional IM Participants.....	3B-12
Figure 23 - Invitation Message	3B-13
Figure 24 – Add Invitees.....	3B-13
Figure 25 - Address Book.....	3B-14
Figure 26 - Sending Invite Message	3B-14
Figure 27 - Impromptu Meeting Room.....	3B-15
Figure 28 - Adding Tools.....	3B-16
Figure 29 - Select Tools to Add.....	3B-16
Figure 30 - Tools option	3B-17
Figure 31 - Sametime Meeting Center.....	3B-18
Figure 32 - Schedule a Meeting	3B-19
Figure 33 - Meeting Details	3B-19
Figure 34 - Sametime Login	3B-20
Figure 35 - Setting Meeting Details.....	3B-21
Figure 36 - Attaching Files for a Meeting	3B-22
Figure 37 - Setting a Meeting Password	3B-23
Figure 38 - Adding the Meeting Tools	3B-24
Figure 39 - Optimize Meeting Performance	3B-25
Figure 40 - Meeting Summary	3B-26
Figure 41 - Scheduled Meeting Room	3B-26
Figure 42 - Attending a Scheduled Meeting.....	3B-27

Figure 43 - Selecting the Scheduled Meeting	3B-28
Figure 44 - Scheduled Meeting Room	3B-28
Figure 45 - Ending a Scheduled Meeting	3B-29
Figure 46 - Completed Meeting	3B-30
Figure 47 - Quick Start Guide	3B-31
Figure 48 - Available Rooms	3C-1
Figure 49 - Main IPWar Screen	3C-2
Figure 50 - Room Tabs	3C-3
Figure 51 - Recieving Text in Non-Active Room	3C-3
Figure 52 - Closing the Active Room	3C-3
Figure 53 - Password Protected Rooms	3C-4
Figure 54 - People within the Room	3C-4
Figure 55 - Collapsing/Expanding Lists	3C-5
Figure 56 - Sending a File	3C-5
Figure 57 - Retrieving Archives	3C-6
Figure 58 - Text Entry	3C-7
Figure 59 - Status Indicator	3C-7
Figure 60 - Changing the Status	3C-7
Figure 61 - Activity Tabs	3C-8
Figure 62 - New Alert	3C-8
Figure 63 - Create New Alert Dialog Box	3C-9
Figure 64 - New Alert Color	3C-10
Figure 65 - Files Tab	3C-11
Figure 66 - Attaching a File	3C-12
Figure 67 - Creating a Note	3C-13
Figure 68 - Note Details	3C-14
Figure 69 - Creating a Bookmark	3C-15
Figure 70 - Search	3C-15
Figure 71 - 0 CAS 2.x Front page	4A-4
Figure 72 - Header	4A-5
Figure 73 - News Entry	4A-5
Figure 74 - Clocks (footer)	4A-5
Figure 75 - Conditions Chart	4A-5
Figure 76 - Menu(s)	4A-6
Figure 77 - Recent Posts Dropdown	4A-6
Figure 78 - New Document Dropdown	4A-6
Figure 79 - Browse Dropdown	4A-7
Figure 80 - Front page Links (bullets)	4A-7
Figure 81 - Library Configuration	4A-8
Figure 82 - Library Selective Replication – Option	4A-8
Figure 83 - Library Form Upload Field with Option	4A-9
Figure 84 - Library Form Upload Field without Option	4A-9
Figure 85 - Library Document Display	4A-9
Figure 86 - Library Form	4A-11
Figure 87 - Library Document Type – HTML	4A-12
Figure 88 - Library Document Type – Text	4A-12

UNCLASSIFIED

ACP 201

Figure 89 - Library Document Type - URL Link	4A-12
Figure 90 - Distribution by Request.....	4A-13
Figure 91 - Library Selective Replication Request Form	4A-13
Figure 92 - Library Selective Replication Status Page	4A-14
Figure 93 - Selective Replication -Distribution by Request Diagram	4A-14
Figure 94 - Selective Replication - Distribution by Request Flowchart	4A-15
Figure 95 - Selective Replication - Optional Distribute to All Diagram	4A-16
Figure 96 - POC Section	4A-16
Figure 97 - POC Service Listing	4A-17
Figure 98 - Rank Listing	4A-18

TABLES

Table 1 - Transmission - Information Content	1-5
Table 2 - Keyword Syntax	3C-11

Uncontrolled Copy When Printed

CHAPTER 1

GENERAL INSTRUCTIONS

OVERVIEW

101. Multinational operations represent a unique challenge to maritime forces in establishing effective Command and Control (C2) support. The traditional primary method for exercising C2 of maritime units operating in multinational task groups has been ACP 127 based formal military messaging. Dramatic and far-reaching changes in doctrine, organizations and technology are altering the conduct of warfare fundamentally and these changes are revolutionizing the information tools that a commander has available to maintain situational awareness, make decisions, and coordinate the application of force.

102. The potential for information technology (IT) tools to improve information dissemination and collaboration has already been recognized and many of these tools have already been incorporated into many of the world's navies. As a result, tactical commanders today have more information on which to base decisions than ever before. Operational Internet Protocol (IP) networks such as CENTRIXS have demonstrated the speed, reach, and richness of information exchange in real-world operations. However, the introduction of these systems has outpaced the Commander's understanding of how best to use them for efficient and effective information management.

103. Whilst formal ACP 127/128 military messaging is a mature C2 tool that exhibits a number of desirable characteristics, including precedence, guaranteed delivery, address management, distribution schema, message integrity, security, non-repudiation, and authentication, many of the networks that provide this form of messaging are over-loaded; and handling timeframes are increasingly resulting in lengthy delays, particularly when utilizing long-haul strategic networks and national gateways. Changes in current policy relating to the use of formal messaging will assist in overcoming many of these problems.

104. The professional and appropriate use of IT can greatly assist the management of all aspects of Multinational Naval Task Group (MNTG) operations. It provides a suite of useful tools that supplement voice communications, formal message traffic, and tactical/operational data systems. The emergence of a growing requirement for information has seen a wider variety of formats, combined with the ability to now deliver these modern IT tools over line of sight (LOS) and beyond LOS bearers within a Maritime Tactical Wide Area Network (MTWAN). These ongoing developments require the implementation of an effective framework, and guidance for the use of these tools within MNTG operations.

BACKGROUND

105. Military Communications Information Systems (MCIS) have traditionally been divided into two general classes: Tactical and Strategic.

- a. Tactical systems are usually self-contained within a command structure and are designed to allow the commander to conduct his mission at the operational level.
- b. Strategic systems are generally more global in nature and are operated on either a common-user or special purpose basis. While a strategic system may be confined within a specified area, it may also be limited to a particular type of traffic.

106. Whilst ACP 121 clearly defines strategic and tactical level communication, modern TCP/IP based communications systems are best situated at the Operational level providing communications services to the Strategic, Operational and Tactical levels. Consequently procedures and doctrine have to be developed in order to support this new paradigm. Future emphasis will be toward direct services between users of computer terminals, in the form of desktop-to-desktop facilities using tools such as chat, e-mail and web services. Furthermore, developments in LOS ad-hoc networking will reduce the reliance on satellite services and enable voice, data, graphics, and video or imagery to be fully exploited at each of the strategic, operational and tactical levels.

PURPOSE

107. To meet and sustain warfighters' messaging requirement, an operational construct that effectively and efficiently employs all available information tools must be sourced. The intent of this document is to provide a "concept" that will meet this requirement. This concept is based on the establishment of an operational doctrine, with integrated lines of authority, processes and tools, that is responsive to all MNTG domains. The objective is an end-to-end tactical command and control capability with integrated doctrine, tactics, techniques and procedures (TTP) that manages and directs tactical messaging at the Task Group level.

108. Collaborative tools, applications and operating systems run on information systems. It is therefore imperative that the efforts of those responsible for managing the information are intimately linked to those responsible for managing the systems and networks, in order to develop the most appropriate collaborative solutions to meet the Commander's needs.

SCOPE

109. Chapter 1 of this publication is designed to provide the basic Concept of Operations for information exchange using IP systems within the context of an AUSCANNZUKUS MNTG, under the tactical command and control (C2) of a designated authority. Chapters 2, 3 and 4 provide more in-depth explanation of the means and use of tactical messaging tools, supported by accompanying annexes that provide the Standard Operating Procedures (SOPs) associated with the use of email, chat and web services.

110. Such a MNTG invariably operates in a bandwidth constrained environment across a Coalition/Allied MTWAN. Whilst most MNTG operations will be conducted on an appropriately covered and secured MTWAN, from time to time it may be necessary for MNTG units to operate in support of specific activities involving external Government and Non-Government agencies.

During these operations there may a requirement to communicate in an unclassified environment using many of the tools specified in this document.

111. This document also provides a high level description of four key attributes of MNTG tactical messaging: Authentication; Confidentiality; Integrity; and Non-Repudiation for both originator and recipient. Other applicable attributes are included in ACP121.

TACTICAL MESSAGING SYSTEMS

112. The aim of this document is to provide guidance on the employment of TCP/IP based tools. Tactical messaging is not restricted to any particular medium or protocol, it includes messaging protocols such as visual (ACP130), voice (ACP125) and teletype (ACP127/128). These methods of communication will continue to be of value to the Commander and their use in conjunction with modern TCP/IP equipment and systems will provide a greater array of information than was previously possible. Wherever possible, interoperability of tactical systems with strategic, combined and allied systems is to be maintained.

113. Additionally, the information and guidance provided in ACP121 (Communications Instructions General) and ACP176 (Allied Naval and Maritime Air Communications Instructions), applies equally to modern TCP/IP systems and will continue to be the accepted standard for the planning and implementation of Allied Maritime communications.

SECURITY

114. ACP 122 provides guidance on Communications Security for the safeguarding COMSEC material and information. All information and resources are to be appropriately safeguarded at all times. Safeguards must ensure that suitable levels of confidentiality, integrity, availability, authentication, and non-repudiation based upon mission criticality, level of required information assurance and classification or sensitivity, are maintained. The safeguarding of information and information systems shall be accomplished through the employment of multi-disciplined defensive layers, as well as sound administrative and operational practices.

115. Procedural aids may considerably enhance Communications and Transmission Security. The degree and duration of security protection afforded by these aids is dependent on their correct use and requires a thorough understanding of their respective capacities and limitations. Abuse or misuse of security aids will quickly compromise their effectiveness and will ultimately, and simultaneously, instill a false sense of security. It is imperative that all operators are conversant with, and are able to apply all measures necessary to protect own and allied forces against interception, analysis and deception.

DEFINITIONS

116. Communications-electronic terms and definitions are contained in ACP 121 and ACP 167. Additional definitions are included below to provide the reader with an understanding of new conceptual terms.

- a. COI – The term Community of Interest (COI) refers to a collaborative group of users within a domain that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information it exchanges.
- b. Tier 1 Network - A coalition capability or application that can be accessed from a national C2 network. At Tier 1, allied nations will exchange information between permanently inter-connected national classified C2 systems over multiple security domains.
- c. Tier 2 Network - A coalition capability or application that is not integrated/connected to national C2 systems and can be accessed from a stand-alone C2 system. At Tier 2, information sharing at all command levels within a coalition or with nations without national C2 systems will be by means of standalone networks and systems.
- d. Web Services - A standardized means of integrating web-based applications using open standards over an Internet Protocol backbone. Web services allow applications developed in various programming languages and running on various platforms to exchange data without intimate knowledge of each application's underlying IT systems.

MODUS OPERANDI

117. In addition to the TG/TF COMPLAN, high-level guidance for Information Management (IM) is normally articulated in the Information Management Plan (IMP). The Operational or Tactical Commander will also stipulate the tactical level IM requirements in an OPTASK IM, including the Information Dissemination Plan (IDP). Delivery of tactical messages within the TF/TG must follow the IDP using the C2 medium specified.

118. The use of TCP/IP based tools is encouraged and should be used wherever possible to facilitate MNTG coordination and reduce voice circuit loading. Many contemporary applications however, have some inherent limitations that make the use of voice circuits the preferred communications path in certain situations.

119. In general, voice circuits should be used to issue orders whilst chat and e-mail should be used to pass information and provide coordinating instructions. There are occasions when critical information must be expeditiously directed to, and acknowledged by, a specific person as opposed to a proxy. Such occasions will also require a high degree of confidence in both sender and receiver identity. While coordination of these types of events may be accomplished via voice, e-mail or chat, executive orders must be passed via the appropriate voice circuit. The conduct of these activities must be clearly articulated prior, by the Commander in the OPTASK IM, taking into consideration information management best practices. Information relating to the order may be passed via chat or e-mail to support and / or reinforce the voice transmission. Orders will not normally be given in a whisper box.

120. ACP 200 Chapter 3 details the types of traffic passed, and the associated means of transmission. This information is reproduced in Table 1 below.

Examples:

- a. ACE1 - indicates that the Commander has approved: Email, Web replication, and ACP127/128 messaging may be used to pass Administrative and Non-Mission Essential Traffic.
- b. G7 – Voice is to be used for all Immediate Action Orders and Coordination
- c. CE23 -Web replication and ACP127 / 128 messaging may be used to pass executive orders, directives, and regularly promulgated updates and summaries.

Transmission		Content	
A	Email	1	Administrative and Non Mission Essential Traffic e.g. PERSTAT, OPDEF, etc.
B	Email with authentication	2	Executive Orders and Directives, e.g. OPGENs, OPTASKs, etc.
C	Web Replication	3	Regularly promulgated updates and summaries e.g., ATO, OPSUM Feeders, OPSTATs etc.
D	Web Replication with authentication	4	Non-regularly promulgated updates and summaries e.g., CCIR, RFI etc.
E	ACP 127/128	5	Rules of Engagement.
F	CHAT	6	TACSIGs IAW ATP1 Vol I article 4124.
G	Voice	7	Immediate Action Orders and Coordination e.g. NGS, track deconfliction, weapon engagements.

Table 1 - Transmission - Information Content

121. In the event that voice communications cannot be established or maintained, an alternate means of communicating time critical orders must be in place. This secondary means of communication should be the use of flash message traffic. If the delay in drafting and transmission of flash traffic precludes the use, chat may be used to issue the order provided it is immediately followed with a flash message. This messages must detail actual date and time that the order was posted, and the identity of the officer issuing the order. All such orders shall be logged.

122. It is important that the Commander determines and promulgates an appropriate means of transmission for the delivery of information, orders and other official traffic. The Commander may also specify release and/or authentication procedures associated with media such as chat and e-mail. For example, the Commander may require the acknowledgement of orders and tasking passed via chat in order to ensure the order is received and understood. It may also be necessary

that, in the case of chat messages, confirmation of receipt of the order / coordination / directions is recorded as an official “Record of Decisions and Orders” promulgated during the chat session.

ELEMENTS OF SERVICE

123. As a consequence of the staged delivery nature of modern electronic messaging systems, there may not be any direct, real-time association between an originator and a recipient. Therefore, many of the functions required to maintain confidentiality, and verify origin and receipt must be performed independently by the originator and by the recipient, based on their respective information. Future messaging systems include certain security features that are applied directly to the message content. These Elements of Service (EoS) include the following:

- a. Authentication. Authentication includes measures designed to provide protection against fraudulent transmission and imitative communication deception by establishing the validity of a transmission or message. Should a Commander require verification of the authenticity of orders received via email or chat, existing authentication procedures laid down in ATP 1 and other tactical publications may be used.
- b. Confidentiality. This function enables an originator to ensure the confidentiality of the content of the message, and assures the recipient that the message content received is identical to that which was sent.
- c. Integrity. Integrity assures the originator that the sent message cannot be modified without the recipient detecting the modification.
- d. Non-Repudiation, for both originator and recipient. This function provides the recipient with evidence of the identity of the originator, and protects against any attempt by the originator to falsely deny having sent the message. Likewise it provides the originator with evidence of the identity of the recipient, and protects against any attempt by the recipient to falsely deny having received the message.

FUNCTIONAL (ROLE BASED) ACCOUNTS

124. Wherever possible, user accounts utilized for the sending and receiving of tactical messages must be role based. All TF/TG units are to maintain a continuous guard on all watch standing or watch keeping accounts utilized for the sending and receiving of tactical messages, including chat and e-mail. A list of common watch standing positions is contained in Annex B to Chapter 2.

MANAGING NETWORK OVERHEADS

125. In an emergency, or during operations when the communications capacity of the network is overloaded, it will be necessary to manage TCP/IP traffic to ensure prompt handling of vital information. ACP 121 specifies the policy and procedures to be followed in order to reduce traffic, and the OPTASK IM details the Commander’s specific requirements in the event of it becoming necessary to implement MINIMIZE procedures on the MTWAN. The order

'MINIMIZE' indicates that it is now mandatory for normal traffic to be drastically reduced, so that vital messages connected with the situation shall not be delayed.

TRAINING

126. The attainment of reliability, speed and security depends, to a large extent, upon the operator. It is essential that the operator is well trained, maintains circuit discipline and understands thoroughly the responsibilities of the position.

127. The effectiveness of any communications system is directly influenced by those it serves. This is particularly relevant where the user operates the terminal from a desk-top station. End-users will only be able to gain maximum benefit from the available services of the system if the individual makes the effort to become familiar with the system capabilities and the relevant procedures.

128. Training and educational programs are essential for providing personnel with the knowledge and skills required to work in a communications environment in an efficient and effective manner, particularly in a Coalition environment.

CIRCUIT DISCIPLINE

129. Compliance with prescribed procedures is mandatory. Unauthorized departures from these instructions invariably create confusion, reduce reliability and speed, and tend to impact the effectiveness of security measures. If the procedure prescribed herein does not address a specific operating requirement, the matter should be brought to the attention of the supervisor.

130. Detailed instructions relating to transmission security should be read in conjunction with this publication. Such instructions are contained in ACP 122.

131. Transmission shall not be made without proper authorisation. The following practices are forbidden:

- a. Violation of radio silence,
- b. Unofficial conversation between operators,
- c. Transmitting in a directed net without permission,
- d. Transmitting the operator's personal sign,
- e. Use of other than authorized prosigns,
- f. Profane, indecent or obscene language.

CHAPTER 2

E-MAIL

BACKGROUND

201. Electronic mail (e-mail) is fast becoming entrenched in operational and business practices and its use as a convenient communications tool continues to increase. Because e-mail lacks the formality of traditional ACP 127 military messaging, it is often perceived as an informal or ephemeral means of communication. Formal military messaging has traditionally provided a reliable and traceable communications system with well-established doctrine for message labeling, authorizing release and clear identification of the addressees required to take action on the content.

202. As the ACP 127 military messaging systems become overburdened and struggle to keep pace with the demands placed upon them, e-mail offers the user immediacy and direct person-to-person contact, while still allowing a documented record of the communication. These benefits are often constrained however, by:

- a. a lack of standard operating procedures for formatting, labeling, release and addressing; and
- b. a lack of assurance of reliability, authentication, delivery or response.

203. In addition, the undisciplined use of this tool often results in critical or actionable information being lost amongst some less important, 'for information only' and conversational e-mails.

SHORTCOMINGS

204. The use of e-mail as means of military messaging raises a number of concerns that must be addressed. Appropriate processes must be put in place in order to overcome these shortcomings.

- a. The relative importance of one e-mail over another is not always readily apparent;
- b. It is not immediately apparent whether an e-mail constitutes an order, intention, request or simply provides information;
- c. Many e-mail systems do not provide guaranteed delivery or acknowledgement of delivery;
- d. E-mail systems rarely offer non-repudiation without the use of additional authentication or encryption systems;
- e. It is not always easy to determine the occasions on which e-mail should or should not be used;

- f. E-mail access will be available to many personnel; therefore e-mails may appear to, but may not necessarily represent the thoughts of the command; and
- g. E-mail can occupy substantial bandwidth, particularly when large attachments are transferred.

RESPONSIBILITY

205. Commanders and managers at all levels are responsible for ensuring personnel under their supervision adhere to the policies contained within this publication.

206. All users are responsible for the use of their respective e-mail accounts and will be held accountable for messages issued in their name. Any use that will knowingly cause congestion on the MTWAN, will unnecessarily waste resources, or will otherwise interfere with the work of others is considered inappropriate.

WHEN TO USE E-MAIL

207. Generally e-mail should be used to communicate non-critical information. Given the store and forward functionality of email, it should not be used for distribution of near real time information or formal orders. The Commander should provide guidance within the IDP regarding information that should be passed by e-mail, and that which should be passed by other means. There will always be occasions not covered in the Commander's IDP where the use of e-mail may be appropriate or necessary, and this remains a decision to be made by local staff and command teams on a case-by-case basis.

208. When using e-mail in lieu of formal messaging, users must ensure that the e-mail:

- a. is released with the authority of a releasing officer who is responsible for the content and correct addressing of the e-mail;
- b. where possible, only uses appropriate watch standing or watch keeping role-based addresses in the From, To, and Cc addresses. Annex B to this chapter provides a list of agreed role-based and watch standing / keeping terms for AUSCANNZUKUS nations;
- c. clearly identifies the point of contact (POC) in the last line of e-mail content or the e-mail signature block; and
- d. includes a precedence marker, acknowledgment request, security classification or other appropriate markers in the standard e-mail format, as detailed in paragraph 210 below.

E-MAIL FORMAT

209. All MNTG e-mail must be drafted in accordance with the following standard e-mail format. Specific elements of the format are amplified in the following paragraphs. Until the

following e-mail format markers are provided as selection options for automatic insertion into the e-mail template, they are to be typed into the subject line, as shown in the examples.

- a. Precedence marker 'URGENT'—used only when appropriate, the word URGENT is placed at the start of the subject line. The default precedence for e-mail on all MNTG networks is 'ROUTINE' and the absence of a precedence marker indicates the e-mail is routine. Unlike formal ACP127 messaging, there are only two precedence levels for MNTG e-mail - ROUTINE and URGENT. See paragraph 210-214.
- b. E-mail subjects should be identified using the naming convention outlined in ACP 200 Chapter 3. The subject should immediately follow the acknowledgment request marker. This uniform naming convention permits easy reference to e-mails at a later date.

Example: INTSUM_21MAY05_N2_C

- c. Releasability indicator marker, e.g. REL AUSCANNZUKUS - used only when appropriate, immediately following the classification marker on the subject line, e.g. INTSUM_21MAY05_N2_C REL AUSCANNZUKUS. Similarly, other caveats (e.g. codewords and special handling instructions) may be included as appropriate.
- d. Privacy marking, used only when appropriate, inside the square brackets after the security classification and any caveats on the subject line.

Example: [REL GCTF-CNFC STAFF-IN-CONFIDENCE].

- e. Drafting officer's name and contact details—only when appropriate and different to the releasing officer, placed after the message content.
- f. Originator/releasing officer's signature block—after the message content. The content of e-mail signature blocks is to be restricted to textual information that amplifies the identity of the e-mail originator. The inclusion of quotations, graphics, pictures, backgrounds, wallpapers, sound files or movie files in signature blocks is an unnecessary waste of bandwidth and is not to be used in MNTG e-mail.
- g. Disclaimer clause - placed after the signature block. The use of a disclaimer is optional on MNTG MTWAN.

PRECEDENCE MARKERS

210. Routine e-mails should be read and action taken as soon as practical. There is therefore no need to include a precedence marker in these e-mails. Routine e-mail should not require action outside of the recipient's normal work hours.

211. Where an e-mail sender requires the recipient to read an e-mail with greater urgency than for routine e-mails, as the subject matter is time-sensitive, they are to include the precedence marker 'URGENT'. The recipients are to read it prior to those that do not contain any indication of precedence.

212. Senders should always consider carefully the relative time zones and normal work hours of addressees before they release an URGENT e-mail, as it may require duty staff to recall action addressees outside of normal work hours. URGENT e-mails should be used sparingly and in similar, exceptional circumstances to when a high precedence ACP 127 formal message would be used. Examples are for time-sensitive information needed for operations, orders with time-limited or critical action requirements.

213. E-mail users are to establish, to the greatest extent allowed by the system they are using, automated and/or manual functions to identify when an URGENT e-mail has been received. A user defined rule or agent that identifies the precedence marker will assist recipients in quickly accessing and prioritising e-mails.

214. Some e-mail applications have facilities to select 'high importance' or 'low importance' tags for e-mail lists, or provide an e-mail options menu that allows high, normal and low importance labels to be placed in the header of e-mails. These should not be confused with precedence, but may be used to assist the reader in further prioritizing e-mail.

ACKNOWLEDGEMENT REQUEST

215. For a variety of reasons, e-mails may not be received, read and/or understood by the intended action addressee(s) within the timeframe expected by the sender. The automatic 'read' or 'return' receipts provided by some e-mail systems cannot be relied upon to indicate that an e-mail has actually been read by the action addressee. If confirmation of receipt of an e-mail is required, the onus for obtaining this confirmation rests with the sender, not the recipient. This is usually achieved via a telephone call, personal visit or a follow-up e-mail. For operational, time-sensitive or business-critical e-mails, such as those considered critical to current operations however, an acknowledgment request may be more appropriate. An "ACK" marker shall be placed in the subject line of email messages requiring an acknowledgement.

ACKNOWLEDGEMENT REPLY

216. The action addressees of an e-mail containing the acknowledgment request marker "ACK" are to respond to the originator by a 'reply with history' e-mail, (omitting unchanged attachments), to confirm that it has been read and understood. The word 'Acknowledged' is to be included at the start of the subject line to replace the URGENT and ACK markers.

217. Information addressees are not to send an acknowledgment unless otherwise directed in the e-mail.

ACTION ADDRESSEES (TO)

218. E-mail drafters should carefully select the addressees that are required to take action on the e-mail content. Only these 'action addressees' are to be included on the 'To:' line of an e-mail. Where there is more than one action addressee, the body of the e-mail must clearly identify the actions required from each. The drafter should consider creating separate e-mails for each action item wherever there might be doubt as to who is responsible for each action.

219. Where possible, only appropriate watch standing or watch keeping role-based addressees should be used in the From, To, and Cc addresses. Annex B provides a list of agreed role-based and watch standing/keeping terms for AUSCANNZUKUS nations.

INFORMATION ADDRESSEES (CC/BCC)

220. E-mail drafters should carefully select only the addressees that actually do need to be informed of the e-mail content. These 'information addressees', who are not required to take any action, are to be included on the carbon copy 'Cc:' or blind carbon copy 'Bcc:' lines of the e-mail. Where there are no actions generated by the e-mail, the 'To:' section of the address is to be left empty.

221. The use of customized in-boxes utilizing 'rules' or 'agents' will improve the user's management of received e-mails.

GLOBAL ADDRESS LISTS

222. The Global Address List (GAL) must be updated routinely to reflect current manning. Individual units are responsible for ensuring their respective address lists are correct. Short notice changes prior to the start of any activity make it difficult to establish and maintain GAL coherency. The IM Plan should promulgate the date by which all address lists should be up to date for the commencement of the operation or exercise.

223. Coalition GALs can easily become out dated due to personnel changes and a lack of administrative updates. A local address book maintained by the user and containing key contacts may be an adequate alternative.

224. Units assigned to operations that necessitate joining an existing Command infrastructure are to ensure that GAL amendments are passed as early as possible before the promulgated INCHOP date to the relevant NOC.

ATTACHMENTS

225. To minimize the inefficient use of bandwidth, and therefore maximize network response time for others, compliance with attachment size limitations specified by the Commander in the OPTASK IM must be maintained.

226. Pictures, video files, graphics or embedded objects must not be attached to e-mails when text can adequately convey the intent of the information.

227. If required to embed objects, such as maps within presentations and documents, the use of bitmap graphics (bmp) should be avoided. A more bandwidth efficient graphic format is jpeg using the minimum resolution required.

228. Consideration should be given to posting the attachment to a website or database for subsequent 'pull' or replication by the mobile unit. The use of web sites to post documents will always be more bandwidth efficient than e-mail attachments. E-mails can then be used to provide shortcuts or links to the information of interest.

229. Wherever possible, attachments should be compression and / or optimized using an appropriate tool such as NXPowerLite.

230. Should there be a requirement to send an e-mail with a large attachment (such as evidence photos from a vessel of interest); it should be broken down into a number of smaller e-mails for transmission.

WEBMAIL

231. WebMail provides a basic e-mail service via an easy-to-use browser-based interface. Annex A provides details of the use of Webmail in the MNTG environment.

ROLE BASED ACCOUNTS

232. Annex B provides a list of agreed role-based and watch standing / keeping terms.

EMAIL ETIQUETTE

233. A guide to e-mail etiquette is at Annex C.

WEBMAIL

INTRODUCTION

1. Lotus Domino WebMail provides e-mail services to approved network users. WebMail provides an easy-to-use browser-based interface that allows users to easily perform basic e-mail tasks using an action bar for quick, context-sensitive access to the most often-used actions. Users can reply to and forward messages with or without attachments, compose either standard HTML or rich-text messages and easily schedule meetings and check recipient availability.
2. In addition, using the Secure WebMail services, the user can invoke any or all of the four key elements of service (EoS) of Authentication; Confidentiality; Integrity; and Non-Repudiation for both originator and recipient as specified in the Messaging CONOPS.
3. WebMail allows users to view and work in a Notes mail database that has been optimized for access using a Web browser. The portlet displays the following functional areas using tabs across the top of the window:
 - a. Welcome (default),
 - b. Mail,
 - c. Contacts,
 - d. Calendar,
 - e. To Do, and
 - f. Notebook.
4. Individual Lotus Domino WebMail databases are created at the NOC during account creation. A copy of these databases (or mail boxes) can be replicated to local Domino servers from the host NOC hub servers in order to allow off-line access.

ACCESSING DOMINO WEBMAIL

5. Users can access WebMail services by browsing to the appropriate CENTRIXS Hub Page and click Login.

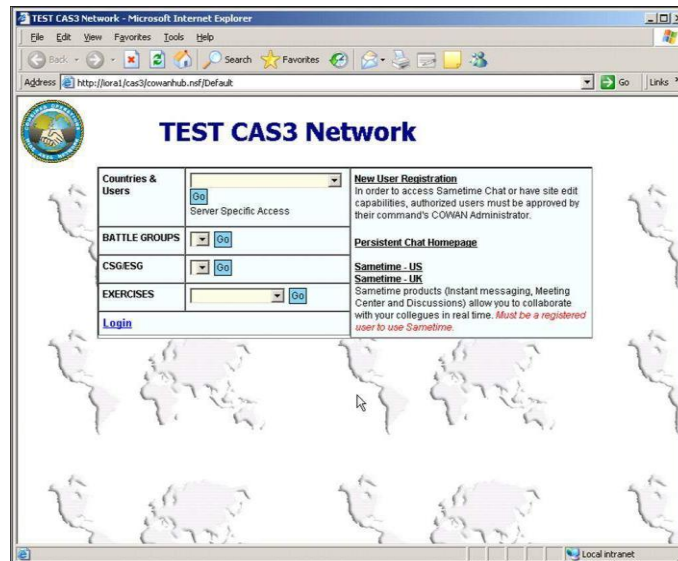


Figure 1 – CENTRIXS Hub Page

6. In the “User Login” window, enter your user name and password and click Login again to enter your enclave's CaS Portal.



Figure 2 - CAS Login Screen

7. On the CaS Portal page, click on the WebMail link to open the Domino WebMail application.

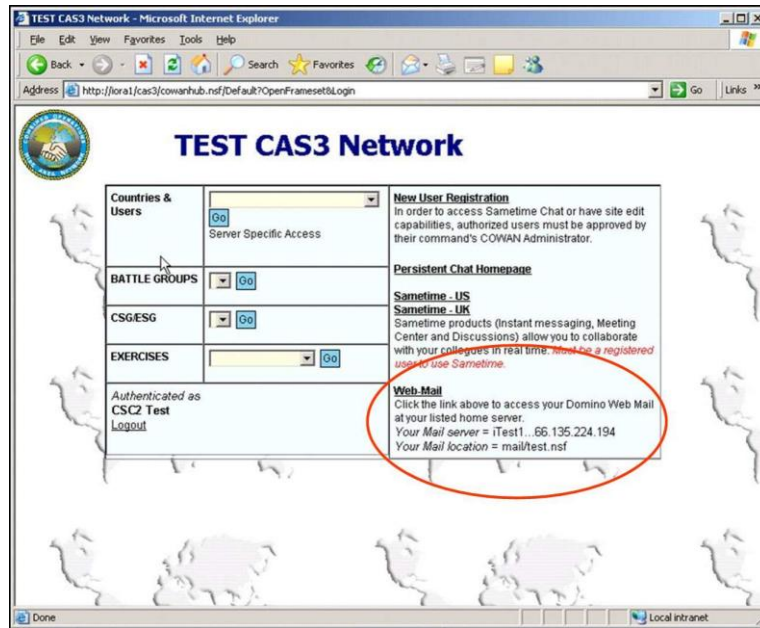


Figure 3 – Webmail Link

8. From the Welcome screen, navigate to the Mail tab on the top of the Lotus Domino Web Access window.

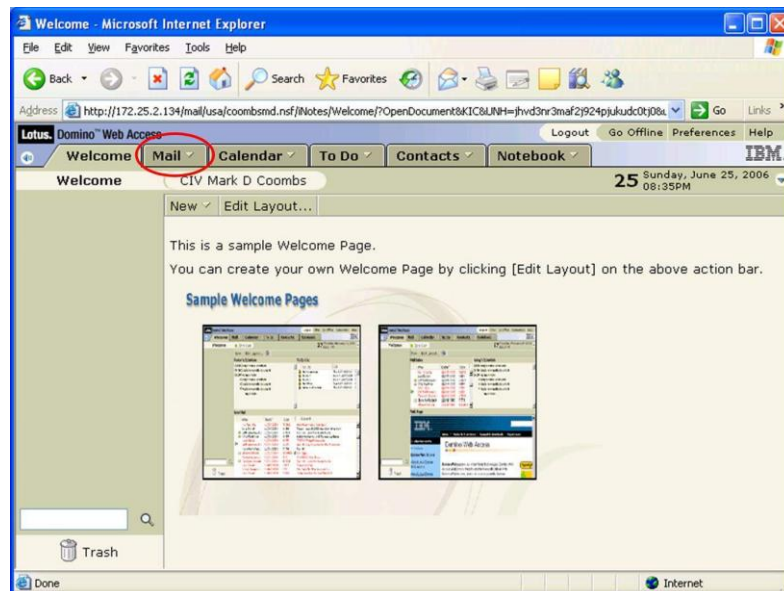
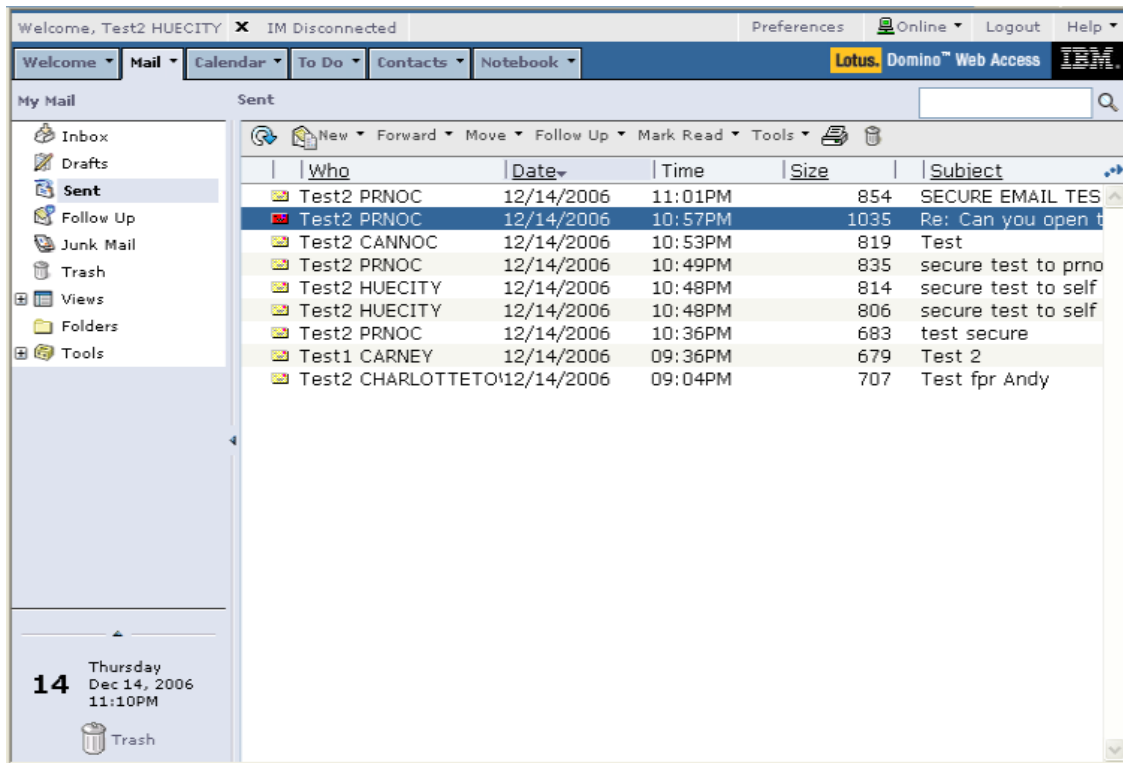


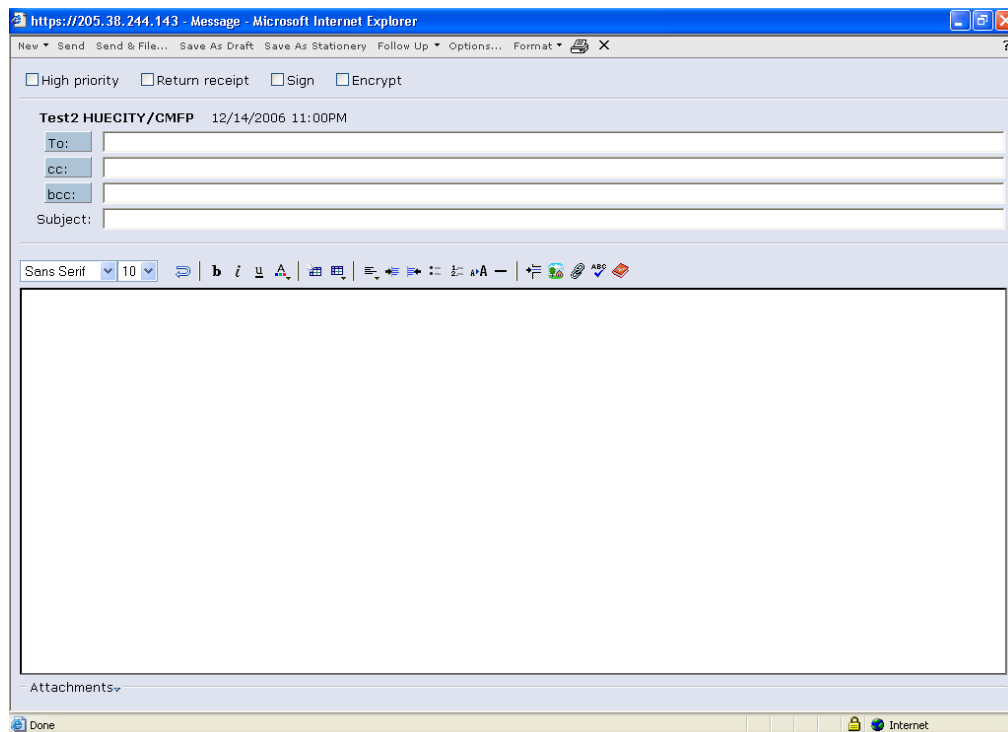
Figure 4 - Mail Tab

9. Use the WebMail application to send and receive and to manage sent and received e-mail using the-mailbox folders within the “My Mail” section on the left of the screen.

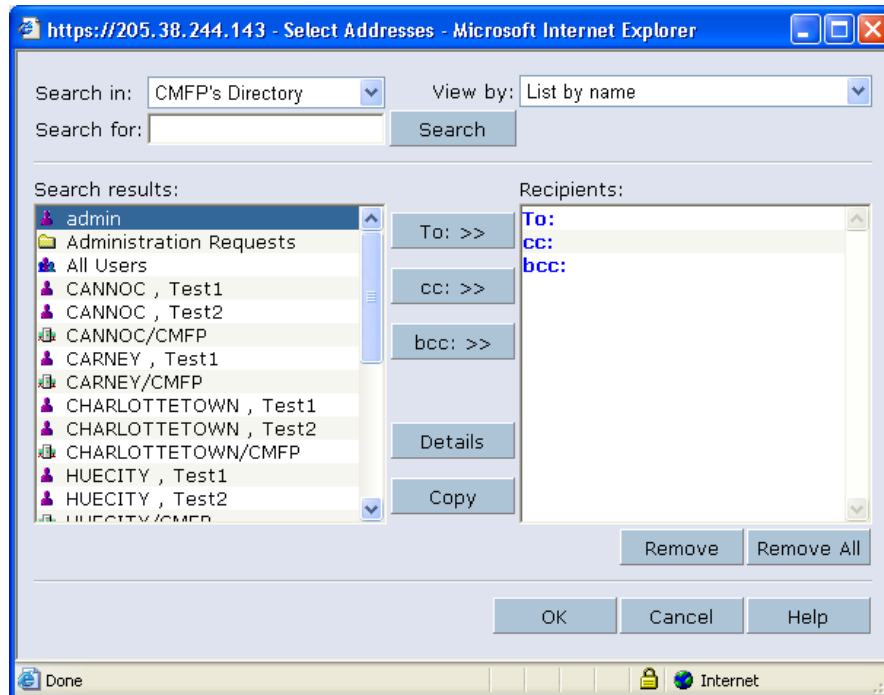


CREATING NEW MAIL

10. To create a new e-mail, click “New” icon  in the-mail toolbar.



11. Users must select appropriate action and/or information addresses to which the e-mail is to be sent. Action addresses are included in the **To:** line and information addressees in the **cc:** or **bcc:** lines. Note: use of bcc addressees should be avoided. Addressees can be added manually or selected from an address book. The address book can be accessed by clicking the To, cc or bcc buttons.



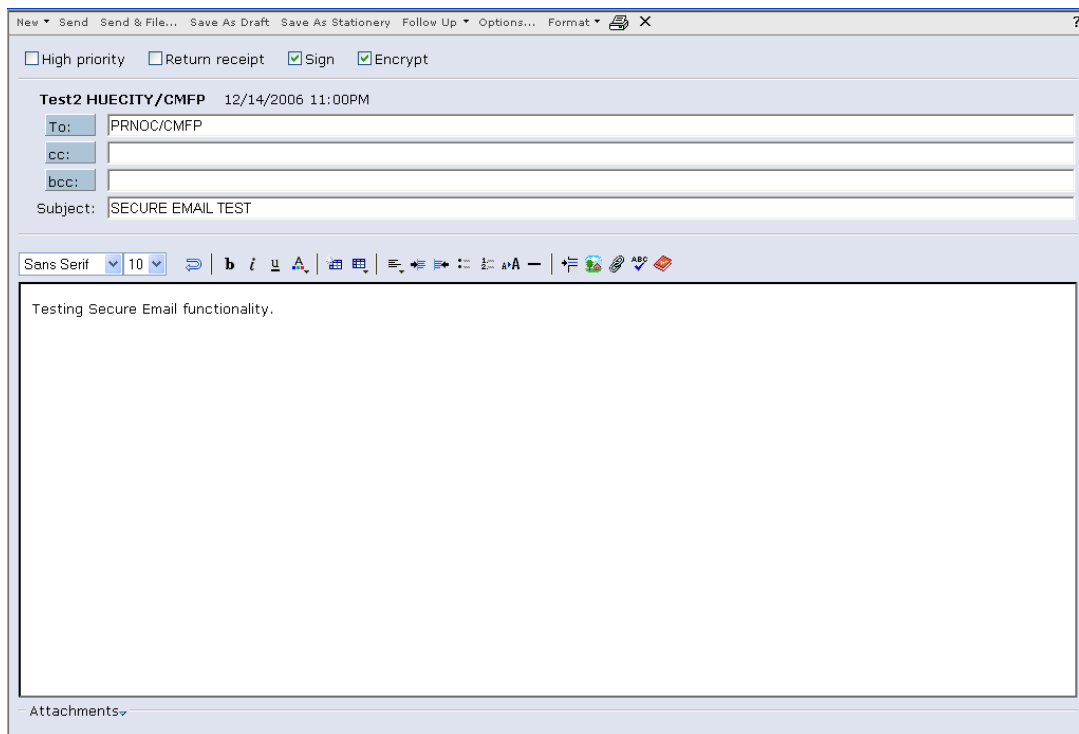
12. Once the addresses have been selected, the user should then insert the subject and text. The subject line should readily identify the purport or content of the text of the e-mail and the text should be concise and contain only information immediately relating to the subject.

13. Attachments can be added to the e-mail by clicking the **Attachments** button at the bottom of the “New Mail” window. All PowerPoint attachments are to be optimized using NXPowerLite 2.4.1. Refer to Trident Warrior 07 Using NXPowerLite StandAlone Version SOP.

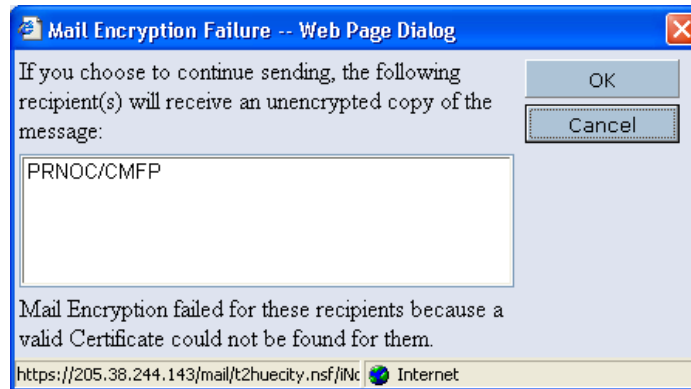
14. The user may use the ☐ High priority ☐ Return receipt ☐ Sign ☐ Encrypt options in the top of the “New Mail” window. These options allow:

- a. High priority - Sets the level of importance so that e-mail recipients can see the indicators in their Inboxes before they open the item. Setting the level of importance also enables the e-mail recipients to sort messages by importance.
- b. Return receipt – Provides the ability to request confirmation that the e-mail was received; and when it was opened.

- c. **Sign** – Provides evidence of the validity of the e-mail, and assures the originator that the message sent cannot be modified without the recipient detecting the modification. It also provides non-repudiation of the e-mail for both the originator and recipient.
- d. **Encrypt** – Enables an originator to ensure the confidentiality of the content of the message, and assures the recipient that content he received is the same as that which the originator sent.



15. When the e-mail is complete and the user is ready to send, click **Send** in the “New Mail” toolbar.
16. At times it may be necessary to send the same e-mail to users who require non-repudiation of the content and those who do not. It is not necessary to originate separate e-mails, rather a single e-mail may be utilized however the following warning message will be received when this occurs.



17. When encrypted or signed e-mail appears in an inbox or sent box, it is identified by a red envelope to the left of the e-mail. The content of the e-mail will not be visible in the preview window.

	Who	Date	Time	Size	Subject
	Test2 PRNOC	12/14/2006	11:01PM	854	SECURE EMAIL TES
	Test2 PRNOC	12/14/2006	10:57PM	1035	Re: Can you open t
	Test2 CANNOC	12/14/2006	10:53PM	819	Test
	Test2 PRNOC	12/14/2006	10:49PM	835	secure test to prno
	Test2 HUECITY	12/14/2006	10:48PM	814	secure test to self
	Test2 HUECITY	12/14/2006	10:48PM	806	secure test to self
	Test2 PRNOC	12/14/2006	10:36PM	683	test secure
	Test1 CARNEY	12/14/2006	09:36PM	679	Test 2
	Test2 CHARLOTTETO	12/14/2006	09:04PM	707	Test fpr Andy

UNCLASSIFIED

ANNEX B TO
CHAPTER 2 TO
ACP 201

EQUIVALENT ROLE BASED ACCOUNTS

Australia	Canada	New Zealand	United Kingdom	United States
Watchkeeper / Watchstander Accounts				
Principle Warfare Officer	Operations Room Officer	Principle Warfare Officer	Principle Warfare Officer	Tactical Action Officer
PWO	ORO	PWO	PWO	TAO
Operations Room Supervisor	Operations Room Supervisor	Operations Room Supervisor	Operations Room Supervisor	Combat Information Center Watch Officer
ORS	ORS	ORS	ORS	CICWO
Communications Watch Officer	Communications Control Room Watch Supervisor	Communications Watch Officer	Radio Supervisor	Communications Watch Officer
CWO	CCRWS	CWO	RS	CWO
Liaison Officer	Liaison Officer	Liaison Officer	Liaison Officer	Liaison Officer

Uncontrolled Copy When Printed

UNCLASSIFIED

ACP 201

LNO_(Cntry code)_(opt. id)	LNO_(Cntry code)_(opt. id)	LNO_(Cntry code)_(opt. id)	LNO_(Cntry code)_(opt. id)	LNO_(Cntry code)_(opt. id)
----------------------------	----------------------------	----------------------------	----------------------------	----------------------------

Principle Warfare Officer(Air)	Surface Warfare Coord	Principle Warfare Officer(Air)	Principle Warfare Officer(Air)	Surface Warfare Coord
AWO	SWC	AWO	AWO	SWC

Principle Warfare Officer(SW)	AntiSub Warfare Coord	Principle Warfare Officer(SW)	Principle Warfare Officer(Underwater)	AntiSub Warfare Coord
PWO(SW)	ASWC	PWO(SW)	PWO(U)	ASWC

Position Based Accounts

Commanding Officer	Commanding Officer	Commanding Officer	Commanding Officer	Commanding Officer
CO	CO	CO	CO	CO

Ship's Comms Officer	Communications Officer	Ship's CommS Officer	Ship's CommS Officer	Communications Officer
SCO	COMMO	SCO	SCO	COMMO

Operations Officer	Operations Officer	Operations Officer	Operations Officer	Operations Officer
OPSO	OPS	OPSO	OPS	OPS

Supply Officer	Supply Officer	Supply Officer	Supply Officer	Supply Officer
SO	SO	SO	SO	SUPPO

Uncontrolled Copy When Printed

E-MAIL ETIQUETTE

1. Although most people give careful thought to what is written down on paper, most e-mails are composed with much less consideration. Off hand remarks and unguarded comments, thoughtless turns of phrase and careless wording can easily create offence or confusion. This miscommunication can be time consuming, costly and in extremis, hazardous in the military environment. Care must be taken when both composing and interpreting e-mail. Irony or humor can be difficult to express in an e-mail message.
2. The following are commercial best practices for the efficient use of staff time and e-mail resources, understanding that recipients of e-mails will be more likely to read and reply to e-mails that can be easily and quickly understood and prioritized:
 - a. Limit each e-mail message to one topic, briefly stating the purpose of the e-mail in the beginning of the e-mail text;
 - b. Give careful consideration in composing an e-mail, as the meaning and tone that is intended at the writing stage may not be the same as that inferred by the recipient, particularly in the absence of body language. Use of all capital letters or all bold font in e-mail text may be considered shouting and should be avoided;
 - c. Write in a concise, professional and ethical manner, as private thoughts may be construed as being representative of the attitudes of your Command or even your Government;
 - d. On shared networks, avoid data transfer and duplication of file storage by using a hyperlink, the directory location, a short-cut or web address within the e-mail for the recipient to access;
 - e. Send e-mails or replies to only those who need to know. Avoid the use the 'reply all' unless all addressees actually need to know;
 - f. If possible, check the properties of group addressees to ensure all persons listed in the group actually need to receive the e-mail;
 - g. Always read through the e-mail from the perspective of the addressees to ensure it is sensible, without ambiguity and that it clearly portrays your intent;
 - h. Think before forwarding someone's e-mail attached (with history) to your e-mail, to ensure it will not cause any damage or embarrassment to the originator;
 - i. If revising or adding to an existing e-mail document, precede the revisions with the author's initials and put comments in a different color so they are obvious to the recipient;

- j. Be courteous, polite and forgiving to those who are not so careful in composing e-mails and seek resolution by telephone or in person if practical, then courteously point them to these guidelines;
- k. Ensure only well known or approved acronyms are used; and
- l. Don't use e-mail for sensitive or emotionally charged issues. Personnel, personal, or work-related issues that have certain sensitivities are best handled with either a face-to face meeting or telephone call.

CHAPTER 3**CHAT****INTRODUCTION**

301. Chat has been adopted at the tactical and operational C2 levels as a key real-time communications tool. Recent operations have highlighted the impact that real time collaboration tools like chat can have on Naval Operations. An inherently flexible communications circuit, chat has been adopted by personnel at the tactical and planning levels in Task Group Operations due to its reliability, flexibility and low bandwidth overhead.

OVERVIEW

- a. Chat is a real time text-based application capable of multi-point data exchanges. Chat can be used to carry on interactive discussions among many individuals, or record meeting notes / action items discussed in a forum for later review. Chat also allows users to have a private side conversation with another person during a group chat session. There are several advantages that chat brings to the MNTG, including the following:
- b. Chat is an immediate, dynamic, and synchronous discussion medium unlike e-mail that is a one-way static form of communication;
- c. Chat is easily learned by new users;
- d. Chat allows clear reports to be sent to superiors and clear direction to be received simultaneously by multiple subordinates. The chat record can be reviewed to confirm information;
- e. Circuits can be quickly established between users in dispersed locations. For example, key personnel can be brought together to discuss events in real time to exchange views and pass guidance;
- f. Chat communications provide a written record of discussion, which can be reviewed. This is particularly useful for reviewing intentions, forwarding information and maintaining a continual historical record;
- g. Chat is a force multiplier that allows planning staffs at multiple levels to coordinate and resolve problems before they develop into larger issues;
- h. Chat can be used to pass large volume reports that would normally congest a voice circuit;
- i. When used correctly, the chat application consumes relatively low bandwidth.

302. The widespread adoption of chat communications is not without its disadvantages however, and these factors must be considered when determining which communications path to use. The disadvantages include the following:

- a. At the tactical and unit level, chat communications are invariably limited by typing speed and accuracy. Some urgent messages will more effectively be passed via a voice circuit;
- b. It is difficult for an operator, particularly a junior one, to monitor both chat and a tactical display simultaneously. Voice nets remain far less cumbersome. During periods of high intensity such as Action Stations, a dedicated chat operator will invariably be required;
- c. The extensive use of chat to pass information between units and command levels results in noticeable difficulty with information flow when chat is lost for extended periods. This effect can be compounded by a hesitancy to pass required information by other means while awaiting the “imminent” restoration of chat services;
- d. Care should be exercised to avoid creating an information gap between those units with a chat capability and those without. Consideration should be given to backing up chat interactions with frequent voice reports in order to keep the MNTG informed. Chat is less likely to offer the broad awareness of the developing tactical situation provided by voice nets;
- e. Multiple conversations can occur simultaneously, which can cause confusion;
- f. Unconstrained use of chat can over-burden limited available bandwidth, which can result server failures;
- g. Experienced users frequently express thoughts in less than complete sentences and make extensive use of abbreviations, which may not be understood by all MNTG participants;
- h. Although inherently reliable, there can be lapses in connectivity as will be the case with other systems reliant upon satellite bearers. Likewise the effects of frequency propagation on RF-IP bearers may also cause lapses in connectivity.
- i. If a user joins a chat session late, or drops out of an existing session, there may be no record of the discussion that has taken place during the period of absence; and
- j. The ability to pass detailed reports and direction in real-time can lead to a perception of excessive supervision at the subordinate levels. The ability to receive information immediately upon request must be tempered with the patience required to wait for the information to become available to subordinates.

CHAT MESSAGE FORMAT

303. MNTG chat is conducted using plaindress, or abbreviated plaindress message format. Like other forms of Allied military messaging, each chat message transmitted will have three parts, these being the heading, the text and the ending. Where necessary the text can be separated from the heading and ending by the use of the prosign “//”, equivalent to the proword “break”.

a. Heading:

- (a) The heading precedes the text and usually consists of called and calling stations. It will normally only identify action addressees, although it may include information and exempted addressees. The standard Allied method of establishing and conducting combined communications is the call sign or address designator of the station(s) called, followed by the call sign of the calling station and separated by the prosign “DE” or the Proword “THIS IS”.

Examples: ANZ de XJ

W this is XJ

- (b) A station or address designator may be classed as any combination of characters or pronounceable words designated for use in message headings to identify a command, authority, unit or communications facility, or to assist in the transmission and delivery of messages. Two letter Warfare Commander identifiers (eg XJ) or three letter abbreviated ship names ie USS HARRY S TRUMAN = HST may also be used;
- (c) The heading may also identify the precedence of the message, date time group and any other additional requirements such as relay responsibilities.

b. Text:

- (a) In addition to expressing the originator's thought or idea, the text may also contain such internal instructions as are necessary to indicate the requirement for special handling or acknowledgement;
- (b) The text may be separated from the heading and ending by the use of two oblique slants “//” meaning Break. This immediately precedes and follows the text.

c. Ending:

- (a) The Message ending includes:

- (A) the time stamp of the message in the form of hours and minutes expressed in digits, and always in UTC zone suffix (Z), unless automatically appended by the application being used;
- (B) any final instructions, such as corrections to the text, requests for acknowledgement (ACK) or additional relay requirements; and
- (C) is concluded with either an invitation for the called stations to transmit, using prosign "K" or proword "Over", or the end of transmission sign using prosign "+" or proword "Out" or the phrase "more to follow" or symbol "...". Every transmission must end with the prosign K or AR as appropriate,

TACTICAL USE OF CHAT

304. Careful consideration must be given when determining which means of communication to use for passing operational and tactical information. This guidance is provided by the Commander in his IDP, and this should be issued in the OPTASK IM.

305. Chat is a useful and widely used communications method; however it is not a replacement for voice nets, particularly for fast moving events when transmission and receipt of time critical information is required. Voice reports build immediate situational awareness not only for the units directly involved, but for all others guarding or monitoring the net. Voice circuits also provide immediate acknowledgement that a report has been received and understood.

306. Chat is best used where line reports or other non-time critical information can be passed in lieu of tying nets for lengthy reports. As the operational tempo increases however, rapid command decision making is required, and voice reports should be the norm.

307. The Commander's IM requirements are promulgated via the OPTASK IM. This document helps to regulate the flow of information. It allows the Commander to provide the MNTG with the necessary direction and authority for which each media type can be used, including chat. It also allows the Commander to promulgate any specific requirements relating to the use of chat and detail the Scheduled Meeting (SM) rooms required for the operation or exercise, including the Moderator and the associated monitoring requirements for each.

MEETING ROOMS

308. There are two standard types of meetings rooms available for use between units of the MNTG – Impromptu Meeting (IM) and Scheduled Meeting (SM) Rooms.

- a. Impromptu Meeting (IM) rooms are the most common form of chat. An Impromptu Meeting (IM) room are non-permanent forums that automatically close once the final participant leaves. They are used for the exchange of

information relating to anything from OTC/warfare commanders' chat exchanges to exchanges of information between equipment technicians, and are commonly used among planning staffs for inter-unit coordination. IM chat exchanges are generally informal and limited in the number of participants.

- b. Schedule Meeting (SM) rooms are a more formal use of chat used primarily for the exchange of tactical and operational level information between units. SM creates a permanent meeting room that remains available for use at all times with or without attendance. This chat allows the establishment of functional rooms where specific information can be exchanged such as Command Room, MIO, and Logistics.

MEETING ROOM MODERATORS.

309. The Moderator conducts the meeting and controls participation during the meeting. Depending upon the application being used, the Moderator can grant and remove permission to draw on the whiteboard, share a screen, control a shared screen, transmit computer audio and video, and start instant meetings from the Participant List. The Moderator is normally the CWC or subordinate Commander that holds the duty that the meeting room supports. The principle duties of the moderator include:

- a. Ensuring that the chat window is established, maintained and clearly identified;
- b. Establishing unit chat priority, should a critical discussion occur that requires traffic from other units in the room be minimized;
- c. Forwarding traffic and reports of interest to higher authority as necessary - usually through cut and paste;
- d. Controlling access to the room;
- e. Ensuring that the official chat record is saved, normally by cutting and pasting to a separate document, should the application in use not automatically record the discussion; and
- f. Enforcing chat room discipline, ensuring that information exchanged in the room remains clear, professional and appropriate.

MEETING ROOM WATCH REQUIREMENTS.

310. The OPTASK IM should specify the watch requirements for particular chat rooms. This will be either 'GUARD' or 'WHENDI'. These watch requirements are taken to mean:

- a. GUARD. The use of 'Do Not Disturb' and 'I Am Away' features is not permitted. Approval to leave a meeting is to be sought from the OTC, appropriate warfare commander, or Moderator; and

- b. WHENDI. The use of 'Do Not Disturb' and 'I Am Away' features is permitted. Approval to leave a meeting is not required although the intention to do so should be advised.

MONITORING CHAT ROOMS

311. If a unit is active in a chat room, then active monitoring needs to be undertaken as it is assumed that all active participants have read and understood the exchanges. It is also counterproductive if a unit is being called and does not answer. Similarly, if a response to a chat cannot be provided immediately, then alternative means of communications should be used.

DIRECTED AND FREE NETS

312. The type of net and method of operation is determined by the operational factors involved.

- a. Free Net – In this type of net, the Moderator authorizes users to transmit traffic to other stations in the net without obtaining prior permission from the Moderator. Free net operation does not abrogate the Moderator's responsibility for maintaining circuit discipline.
- b. Directed Net – In this type of net, stations obtain permission from the Moderator prior to communicating with other stations in the net. Permission is not required for the transmission of FLASH messages, which shall be sent direct. Transmissions on a directed net may also be accomplished in accordance with predetermined schedules.

313. A chat room is deemed to be a free net unless otherwise ordered. Where there is a requirement to change from a free net to a directed net, or vice versa, one of the phases "THIS IS A FREE NET" or "THIS IS A DIRECTED NET" shall be used by the Moderator.

THE EXECUTIVE METHOD

314. Chat should not be used to pass messages employing the Executive Method. The Executive Method is used when it is desired to execute a tactical message at a given instant; that is, to ensure that two or more units take action simultaneously. As indicated earlier, although chat is inherently reliable, there can be lapses in connectivity as satellite antennas attempt to maintain satellite lock onboard a ship that is manoeuvring.

315. Chat may be used to pass tactical messages taken from a signal book that do not employ the Executive Method. In this case the rules for the use of TACSIGs (ATP1 Vol I Chapter 4) are to be used. Such messages must have a time group included in the message ending.

OPERATING RULES

316. The following rules for chat discipline are mandatory on all circuits. Every station must adhere to the following:

- a. Always:
 - (a) Use correct chat procedure;
 - (b) Maintain a constant chat watch unless specific instructions or permission has been received to the contrary. This requires that at least one person be nominated to monitor the chat window regardless of the circumstances. All aspects of tactical chat procedure are based on the assumption that stations will respond to the call immediately;
 - (c) Answer calls without delay;
 - (d) Wait until the other party has finished typing prior to answering; and
 - (e) End transmissions with either K or +
- b. Never:
 - (a) Violate silence, except in accordance with predetermined instructions for breaking radio or electronic silence;
 - (b) Breach minimize procedures on TCP/IP circuits;
 - (c) Compromise classified information by using unauthorised plain language disclosure when operating on an uncovered network;
 - (d) Make unnecessary or unduly long transmissions.
 - (e) Engage in unofficial conversation or operator's banter; or
 - (f) Identify an individual, ship or unit by name, or any other personal or individual sign when operating on an uncovered network.

BREVITY

317. The need for brevity and clarity in message preparation cannot be over emphasized. To avoid misinterpretation and subsequent explanation, the message must state exactly what is meant and must not be vague or ambiguous. To this end, all unnecessary words may be eliminated. Commonly used conjunctions, prepositions and articles such as AND, BUT, FOR, IN, ON and THE may be eliminated unless essential to the meaning.

- a. **Abbreviations.** Many abbreviations are so commonly used in normal speech they are more familiar than their original unabbreviated form. The use of such abbreviations in chat is encouraged provided that:
 - (a) They are quicker and easier to use than the full word;
 - (b) They are sufficiently well known to avoid any confusion and subsequent confirmatory transmissions; and
 - (c) Where an abbreviation has more than one meaning, the intended meaning is obvious to the addressee from its context or frequent usage.
- b. A list of common abbreviations adopted for MNTG use are included at Annex A to this Chapter.
- c. **Brevity Codes.** A brevity code is a group of numbers and/or letters that equate to a standard predetermined vocabulary of words or phrases, equipment and commodity codes for example. Brevity codes can reduce long stereotyped sentences or lists to a few characters and save considerable time in transmission. It is however important to understand that such codes provide no security at all and must be regarded as the equivalent of plain language when transmitted.
- d. **Punctuation.** Punctuation is not used unless essential to the sense of the message.
- e. **Phonetic Equivalents.** When it is necessary to include isolated letters in messages, the phonetic equivalents should be employed. It is inadvisable for message drafters to employ the phonetic equivalents for single letter words.

AUTHENTICATION

318. When authentication is required, it will be carried out in accordance with the authentication system and policy in force at the time (see ATP1 Vol 1 Chapter 4).

ACKNOWLEDGMENT OF MESSAGES

319. An acknowledgment is a communication indicating that the message to which it refers has been received and the intent is understood by the addressee. A request to acknowledge means "An acknowledgment of this message (or message indicated), when understood, is required" and may be included in the original transmission or passed by separate message.

Example: All ships de XJ // Sitreps required by 1200Z. CHA Ack.

320. An acknowledgment should not be confused with a reply or receipt. It is the prerogative of the originator to request an acknowledgment to a message from any or all

addressees in receipt of that message and only a message including the word “acknowledged” can be accepted as an acknowledgement.

VERIFICATION

321. Under certain conditions, addressees of a message may wish to verify with the originator, the content of the message or a portion thereof. This may be done by chat however, it is emphasized that only an addressee may request a verification, and the reply thereto must be authorized by the originator of the message in question. Operators are not permitted to originate a request for verification or reply thereto.

GENERAL OPERATOR TECHNIQUES

- a. **Tone.** In the case of chat, it is difficult at times to appreciate the tone of a chat message. Tone must be monitored and moderated. It has become common intranet chat protocol for example to express displeasure or shouting through the use of capital letters. Accordingly, use of capital letters for whole phrases or complete sentences is discouraged, although it should be noted that it is common practice for some nations to use all capitals for ships’ names, abbreviations, and phonetic spelling.
- b. **Long Messages.** Sometimes it is preferable to separate prolonged discussions into a number of smaller segments. This ensures that the receiver has the opportunity to consider the information being passed while the sender continues typing. A series of three or more periods (...) should be used to denote a break in a chat segment with further information to follow.

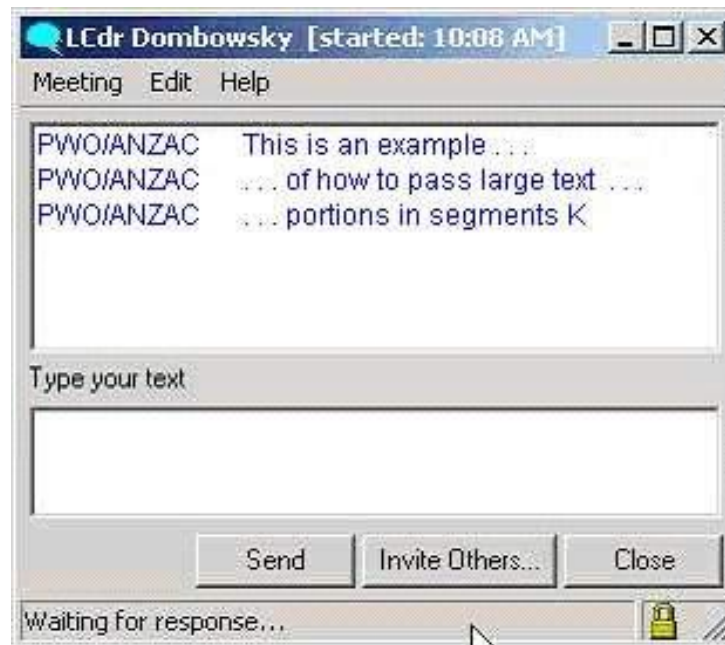


Figure 5 - Example of Long Chat Message

- c. **Operator Identification.** Participants in chat rooms should be identified by position rather than the individual. This may be accomplished by the use of the position designator followed by the three letter abbreviation of the unit, separated by an oblique slant.

Example: The Sametime user PO Smith/ANZAC might be identified as ORS/ANZ.

- (a) When a unit is entering a SM from a meeting schedule, the user should be asked how the name is to appear. This is the opportunity to personalize the chat identity.
- (b) The identification can also be used in the heading of the message:

Example ORS/ANZ de XJ // INT Sitrep // 2305Z K

- d. **Loss of Connectivity Procedure.** Should a unit lose connectivity, any other participant noticing is to make an appropriate entry, annotated with the time in Zulu. Upon reconnecting and returning to the meeting room, units should re-identify themselves, and indicate the time that connection was lost, and the time at re-connection. If persistence is not available, a transcript of the missed chat may be requested from the Moderator.
- e. **Time stamping.** Should an application be used that does not automatically timestamp all transmissions, formal reports and orders passed in chat rooms should be followed by a timestamp. This will facilitate ease of reference and serve as a record of the event time. Time stamps are to appear in ZULU in the message ending, immediately prior to the end of transmission sign (K or +), and separated from the text by a double backslash.

Examples:

HST de XJ // Report status of repairs to main armament // 1230Z K

XJ de HST // ETR unknown. OPDEF to follow // 1231Z +

- (a) Wherever possible, an application that provides persistence and automatic time stamping such as Persistent Chat is to be used.
- f. **Standard Reports.** Standard reports or frequently used templates may be first saved as text files, then updated and copied into Chat as required in order to reduce typing time and errors.
- g. **Recording chat.** SM chat is normally recorded on the server. It may however, be necessary to record a chat session by copying it to a word-processing document or text file and archiving it for access at a later date, particularly where significant events occur and the meeting will continue to be open. Commands should consider the requirement to archive information as directed

in extant instructions. In all cases, where information is passed on IM chat that is considered require archiving, this information is to be copied to a separate text document and archived appropriately.

- h. **Online Status.** Online status is the current active status of a person within a chat room. Status is represented by various icons and colored text and can be one of the following:
 - (a) Offline. Unavailable for chat
 - (b) Active. Logged on and available for chat
 - (c) Away from the computer. Logged on, but away from the computer, leaving a customizable away message. If a message is sent to an address that has an "Away" status, the message will be displayed on the recipient's screen and an automatic response defined by the recipient, will be forwarded to the message originator.
 - (d) Not using the computer. Logged on, but has not touched the mouse or keyboard for a defined time. If a message is sent to an address that has a "Not Using the Computer" status, the message will be displayed on the recipient's screen, and an automatic response defined by the recipient, will be forwarded to the message originator.
 - (e) Do not disturb. Logged on, but does not wish to be disturbed, leaving a customizable message. If a message is sent to an address that has a "Do Not Disturb" status, the message will not be displayed on the recipient's screen, however an automatic response defined by the recipient, will be forwarded to the message originator.

CHAT APPLICATIONS

LOTUS SAMETIME

322. IBM Lotus Sametime is the primary MNTG Chat tool. Sametime has been demonstrated to operate effectively within a maritime low bandwidth environment. Importantly, it also provides the functionality required to support collaborative planning in a single integrated window. Combined with specific applications designed to improve and / or provide enhancements designed to address the shortfalls of the "off the shelf" implementation of Sametime, the application is able to meet the operational requirements of Distributed Collaborative Planning (DCP) for the war fighter at sea.

323. Annex B contains details for the operation of the Sametime suite of tools.

PERSISTENT CHAT

324. Chat is a synchronous real-time system. If a user joins a chat session late, or drops out of an existing session, there is no record of the discussion that has taken place during the period of absence. Instant Persistent War Room (IPWar) is a tool used in conjunction with Sametime that allows users to retrieve chat conversations within a chat room, in order to review information previously passed.
325. Also known as PChat, instructions for the use of IPWar is included in Annex C.

CHAT ABBREVIATIONS AND ACRONYMS

1. To speed the flow of information in a chat room, a number of common abbreviations have been informally adopted. These are a combination of tradition communications prosigns/prowords and some of the modern internet abbreviations that are appropriate for MNTG usage:

AA	All After
AB	All Before
Ack	Acknowledge or Acknowledged
Affirm	Affirmative
AR or +	This is the end of my transmission to you and no response is required or expected; Out
AS	Wait.
att	At this time
brb	Be right back
btw	By the way
cow	Check other window (when two windows are open)
DE	This is
disr	Disregard this transmission
fyi	For your information
INT	Interrogative
J	Verify with originator and repeat.
K	"Invitation to transmit" or "This is the end of my transmission to you and a response is necessary."
mf	Message For
nlt	No later than
R	Roger (this is used to acknowledge receipt of a message, but should not be interpreted as 'Approved')
SB	Stand By, see also AS
SEPCHAT	Separate Chat
WA	Words After
WB	Words Before

SAMETIME

INTRODUCTION

1. Sametime consists of client and server applications that enable a community of users to collaborate in real-time online meetings. Members of the Sametime community use collaborative activities such as presence, chat, screen sharing, and a shared whiteboard to meet, converse, and work together in instant or scheduled meetings.

SAMETIME CHAT

2. The Sametime Chat client is a small chat client used primarily for point to point communications between two or more individuals. Sametime also incorporates the shared workspace function in its Meeting Centre. The purpose of Sametime is not to replace traditional communications tools, but to expand the user's reach and improve internal and external communications within the organization.

LOGGING ON TO SAMETIME CHAT CLIENT

3. To launch Sametime Connect
 - a. Click **START** from the desktop taskbar.



Figure 6 - Sametime Connect

- b. Click **Sametime Connect** from the start menu. This will open the **Log On to Sametime** dialogue box.



Figure 7 - Login Screen

- c. Enter the Sametime user name and password into the appropriate text boxes
- d. Click **Log On**.



Figure 8 - Activity Status

4. The Sametime Group view will appear. The **“I Am Active”** status indicator displays that the user has logged on successfully. This is also known as the user’s “Buddy List”.

LOGGING OFF

5. In Sametime Connect, click People then Log Off from Sametime™ from the menu bar.

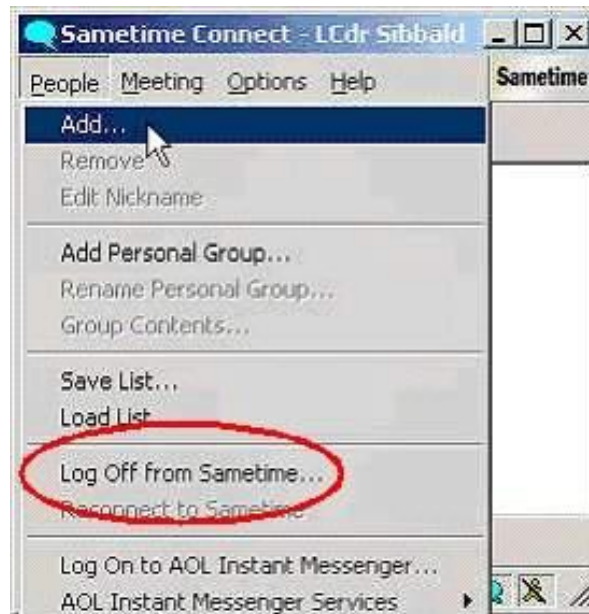


Figure 9 - Logging Off Sametime Connect

LOGGING ON AS A DIFFERENT USER

6. In Sametime, click **People** then **Log Off** from Sametime from the menu bar.
 - a. Click **People** then from the menu bar to go to the **Log On to Sametime** dialogue box.
 - b. Enter the new Sametime user name next to User name.
 - c. Enter the new user's Sametime password next to Password.
 - d. Click **Log On** to go to the Sametime Connect user view.

CONNECT LIST

7. A Connect List is a list of people and groups in Sametime Connect. The list is created by adding and removing people and groups from the Directories. Sametime Connect allows the user to create as many Connect Lists as needed, save them, and load them at any time. The Connect List can also be transferred to other people, and they can log on to Sametime Connect and use your Connect List.

CONNECT GROUPS

8. The Connect List contains two basic kinds of groups: personal and public:

- a. Personal groups are groups of people that are defined by a user. The user controls the membership of his/her personal groups, with the ability to add members from the Navy Address Book.
- b. Public groups are groups defined in the Navy Address Book. The membership of the public group is defined and controlled by system administrators.

ADDING USERS TO PERSONAL GROUPS

9. To add contacts to a Personal Group, select '**Add...**' from the drop-down menu under '**People**'.

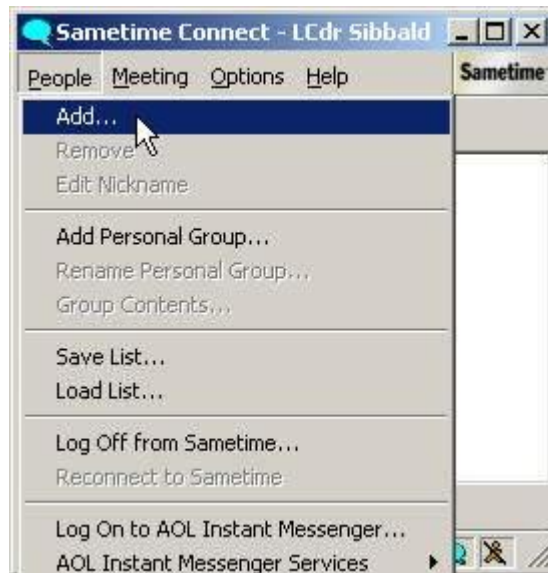


Figure 10 - Adding Users to Personal Groups

10. The "**Add Person or Group**" window will appear.



Figure 11 - Add Person or Group

11. **'Work'** is the default group name; this may be renamed if necessary
12. Users can be added to this group in the 'buddy list' by typing in the username issued to them in the **'User name'** field, or by searching through the Address book. To add users from the address book:
 - a. Select the **'Directory'** button

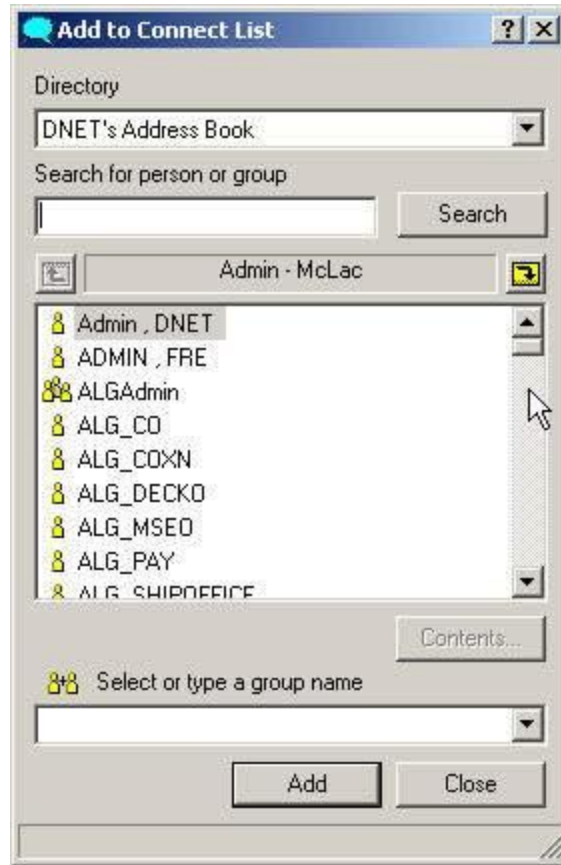


Figure 12 - Directory Listing

- b. The 'Add to Connect List' window will appear
- c. Searching can be performed by scrolling alphabetically or by using the 'Search' button. The search function finds the closest match to the name entered.



Figure 13 - Selecting/Adding Users

- d. Once the desired name has been identified on the list, **'double-click'** it or select it and click on the **'Add'** button and it will be added to the personal 'buddy list.'



Figure 14 - Personal Buddy List

13. An unlimited number of users can be added to an individuals 'buddy list.'

ADDING STAFF GROUPS

14. Various staffs and Sametime User groups (STUserGroupName) are listed in the Address books. This is a quick and easy way of adding an entire group of names into a 'Buddy List.'

- a. To add staff groups to your 'buddy list' Select '**People** ☐ **Add.**'

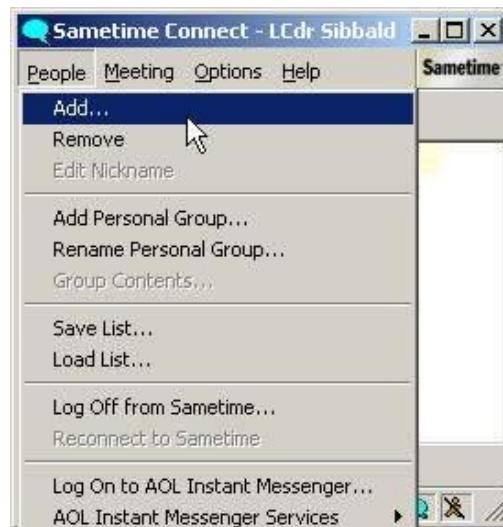


Figure 15 - Adding User Groups

- b. Type in the name of the group or select one or more from the address book,

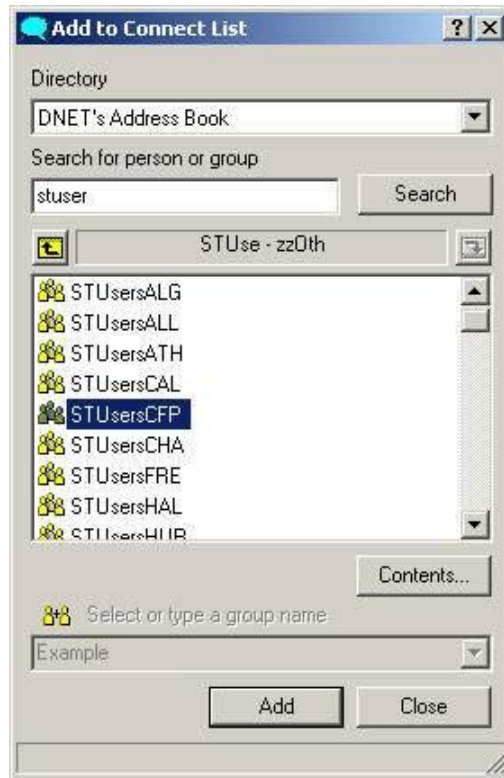


Figure 16 - Selecting/Adding User/Staff Groups

- c. Select the '**Directory**' button.
- d. Search the Address Book for required group.
- e. Staff groups use a different icon than individual user icons.



Figure 17 - Group Contents

- f. Group members can be viewed by selecting the '**Contents**' button.
- g. Once the appropriate group is highlighted, click '**Add**'

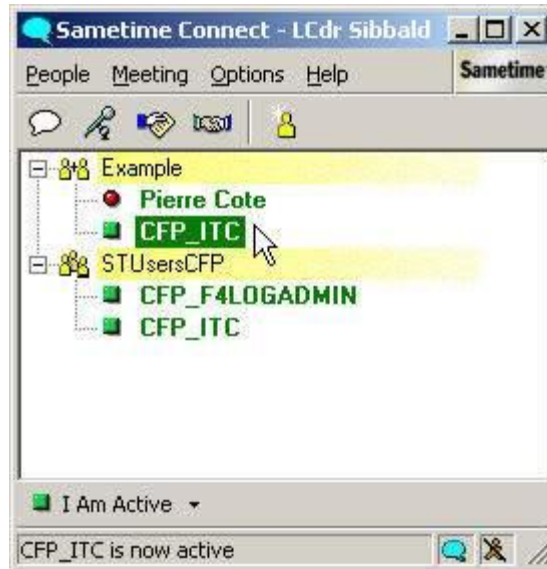


Figure 18 - Staff Groups in Buddy List

15. Staff Groups cannot be modified in the way that personal groups can. Only Administrators can modify staff group contents. It is possible to can drag and drop users from staff groups into private groups – but not the other way round.

USE OF CHAT - TYPES OF MEETINGS

16. As indicated in Chapter 3, chat sessions are conducting in meeting rooms. There are two types of meeting rooms available for use between units of the MNTG – Impromptu Meeting (IM) and Scheduled Meeting (SM) Rooms.

IMPROMPTU MEETING (IM) ROOM

17. To initiate an IM room, ‘double-click’ on the desired user’s name from the ‘buddy list.’

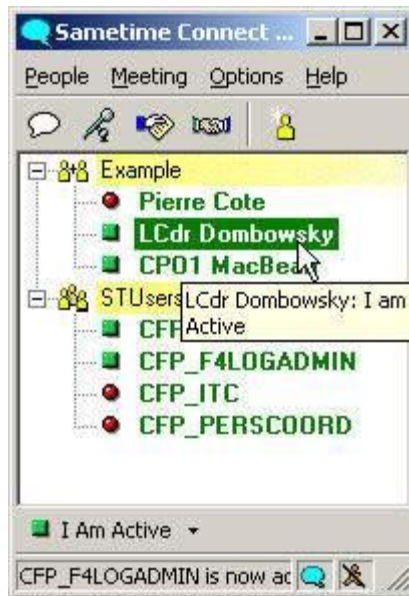


Figure 19 - Creating an Impromptu Meeting Room

18. The 'Send Message' dialog window will appear.

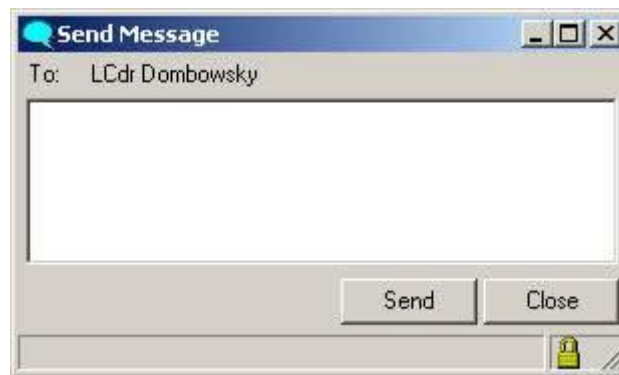


Figure 20 - Message Box

19. Type an appropriate message to invite the user into the chatroom, then click on the 'Send' button.
20. The actual message is not transmitted until you hit the 'Send' button or press the 'Enter' key.

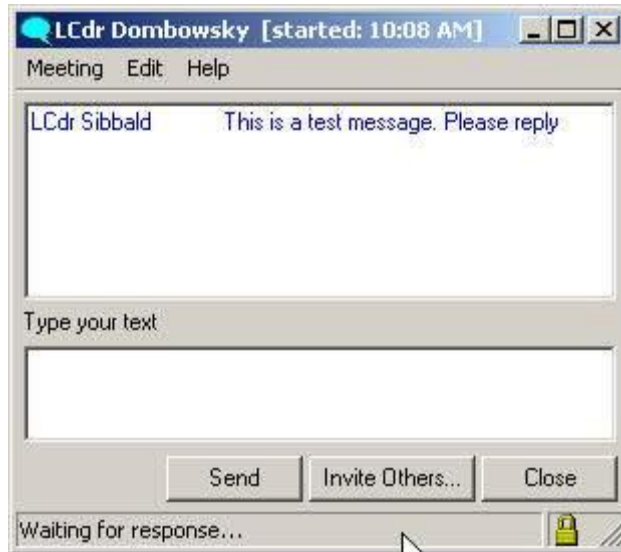


Figure 21 - Chat Window

21. The 'Send' window automatically switches into a chat window and an Impromptu Meeting has been initiated.

INVITING ADDITIONAL IMPROMPTU MEETING (IM) CHAT PARTICIPANTS

22. To invite additional participants into an existing IM room:



Figure 22 - Invite additional IM Participants

- a. From the IM chat text screen, Select **Message | Invite Others...** or click on the **'Invite Others'** button.



Figure 23 - Invitation Message

- b. The '**Invitation Message**' window will appear. Amend the invitation message as required.
- c. Click on the '**Add Invitees**' button or drag from the 'buddy list' to the 'Invitees' field in the 'Invitation Message' window.



Figure 24 – Add Invitees

- d. From the '**Add to Invitation**' window, select a username from the '**Directory**'.

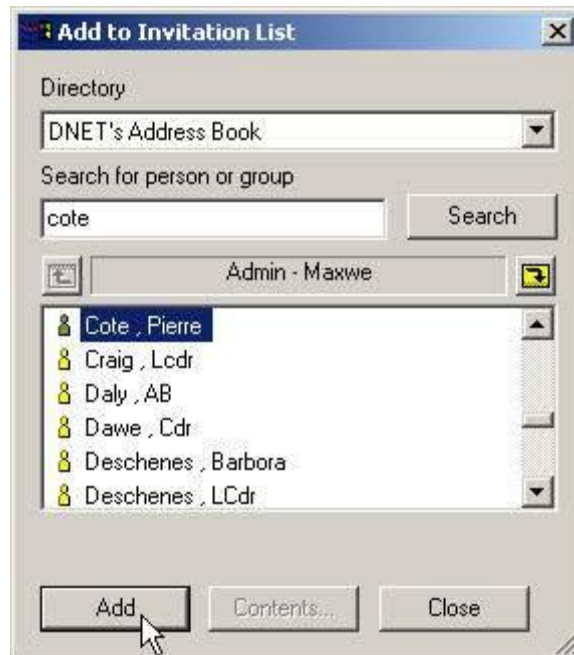


Figure 25 - Address Book

- e. To add the user, **'double-click'** the desired name or click **'Add'** button. Continue to add more people to the **'Invitees'** field as required.



Figure 26 - Sending Invite Message

- f. Once the desired number of people have been added to the IM Chat invitation, click the **"send"** button.
23. The user(s) that the invitation was sent to will receive a message inviting them to join the IM room.



Figure 27 - Impromptu Meeting Room

24. Once a new user has accepted the invitation to participate, the user's name will automatically join the IM room.
25. Whenever a third person is added to an IM room, the Chat window will expand automatically in order to add a **'Participants'** list to the right of the window.
26. Any number of users can participate in an IM room.

ADDING TOOLS TO AN IMPROMPTU MEETING (IM) ROOM

27. Additional real-time collaboration tools (White boarding, Screen Sharing, Audio, and/or Video) may be added to any IM room however an IM room can only be upgraded once with additional tools.
28. Close consideration must be given to bandwidth before upgrading collaboration tools in an IM room. Some tools may not be available on the MTWAN due to bandwidth restrictions



Figure 28 - Adding Tools

29. In order to add tools to an IM room click on '**Meeting | Add Tools**'



Figure 29 - Select Tools to Add

30. Select the tool(s) desired to be included in the upgraded meeting by clicking in the 'check box' next to the tool.
31. Click on the '**Send**' button to launch the upgraded meeting.

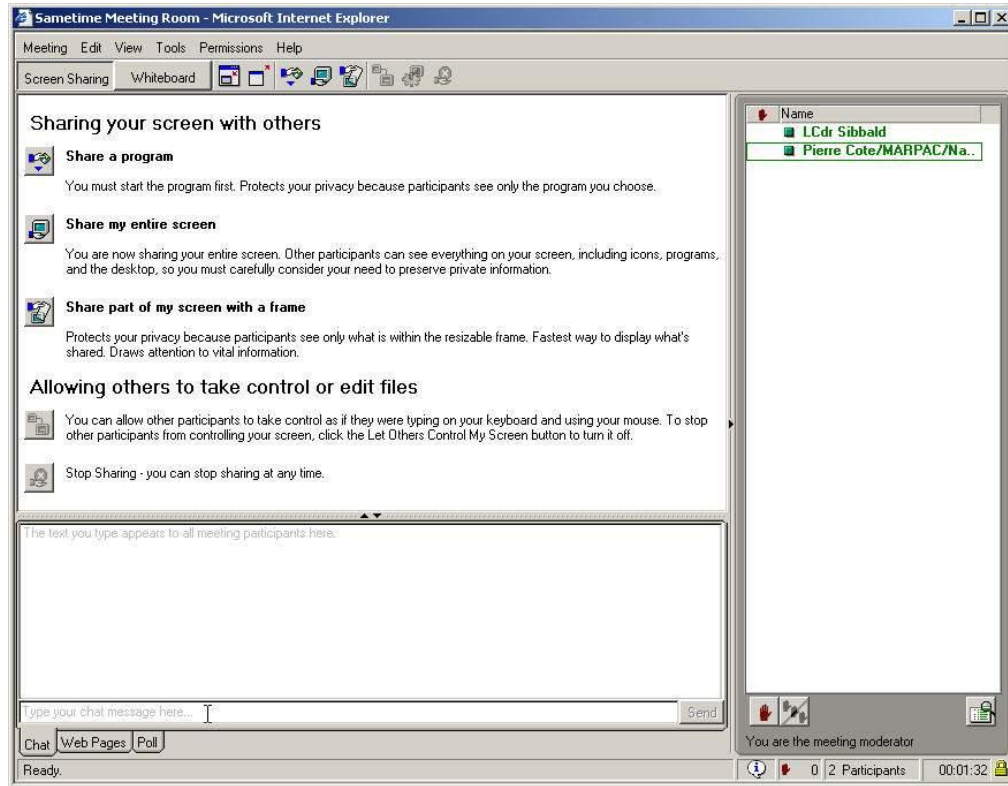


Figure 30 - Tools option

32. The upgraded meeting uses Java Applets, which must be downloaded into your browser prior to the meeting starting correctly. These are the same applets that a Scheduled Meeting Room uses.

33. It is highly recommended for MNTG units to ensure that these Java Applets are downloaded and installed on every workstation while the ship is connected to a high-speed connection. Downloading these applets (approx 4MB) while at sea over limited bandwidth is NOT recommended.

SCHEDULED MEETINGS (SM) ROOM

34. Scheduled Meetings must be initiated using the web based interface of Lotus Sametime, known as the 'Sametime Meeting Centre' (SMC).

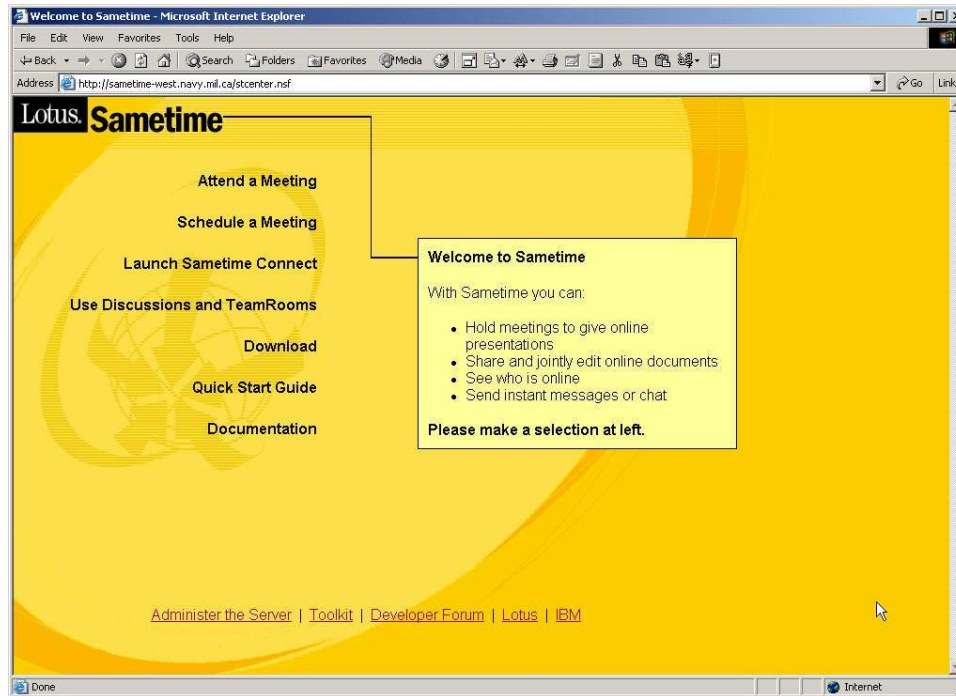


Figure 31 - Sametime Meeting Center

35. In order to get to the Sametime Meeting Center; open the Internet Browser and type the URL for SMC as detailed in the OPTASK Net, or to the local Sametime server if operating in a distributed architecture.

Click ‘Schedule a Meeting’

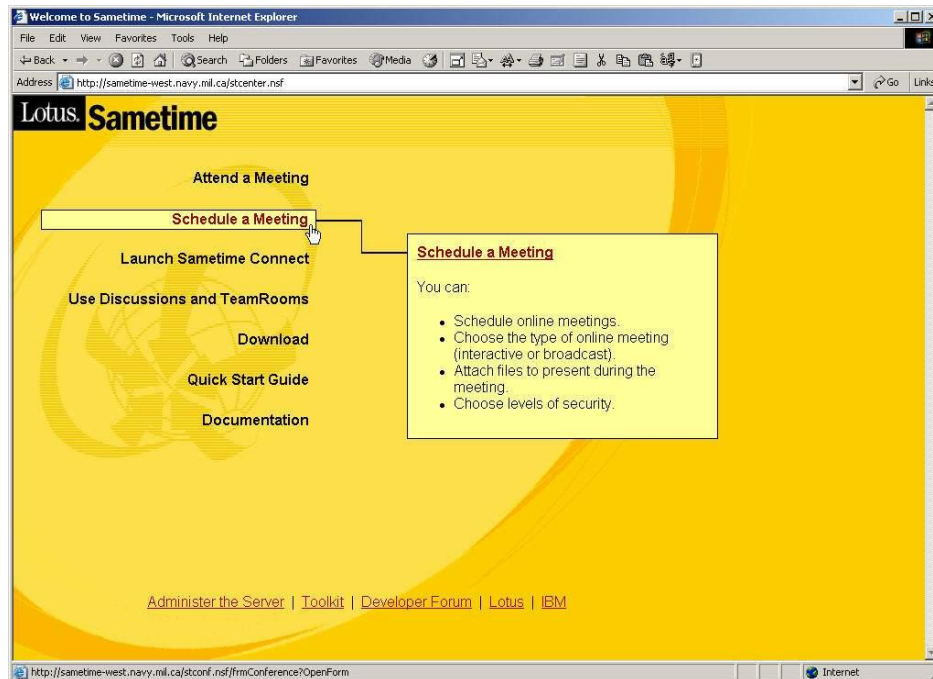


Figure 32 - Schedule a Meeting

36. This will bring you to the **New Meeting** planning tool, requiring the user to log on to Sametime.

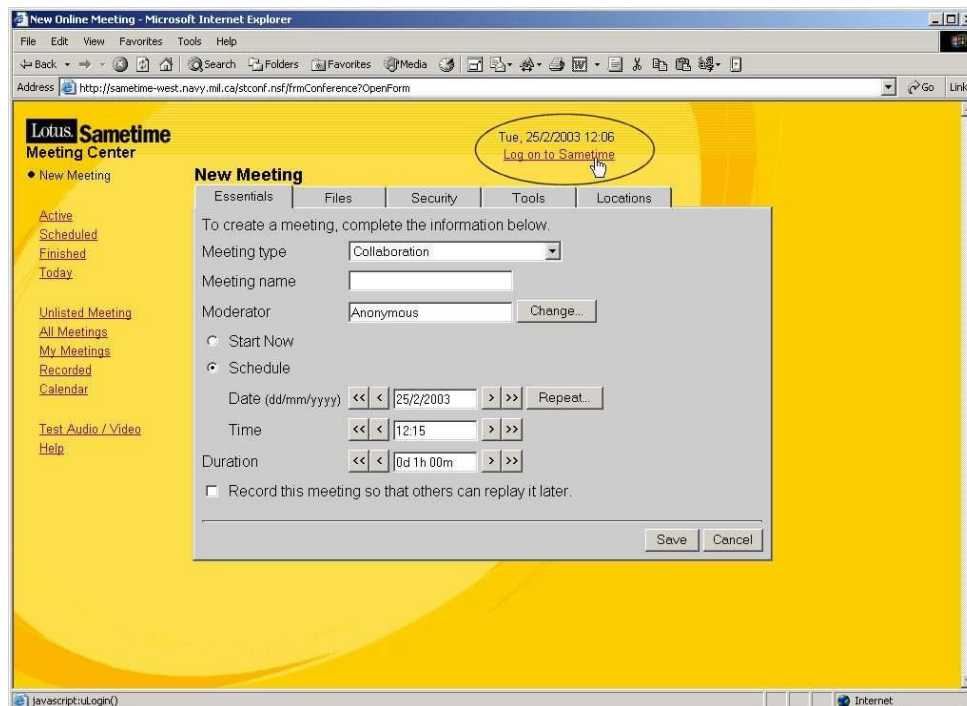
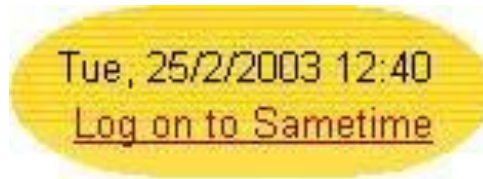


Figure 33 - Meeting Details



37. Click on the red “**Log on to Sametime**” to bring up the Login Page.
38. **Log on to Sametime** using the same User Name and Password for Sametime Connect.

A screenshot of a web page titled "Server Login" in a large, bold, black serif font. Below the title, the text "Please enter your Username and Password" is displayed in a smaller, black, sans-serif font. There are two input fields: "Username" with the text "Lcdr Sibbald" and "Password" with a masked password "*****". Below the fields is a "Login" button.

Figure 34 - Sametime Login

39. If the user chooses not to log on to Sametime, the moderator for the SM shall be listed as Anomyous.
40. The New Meeting planning tool is divided by five tabs: Essentials, Files, Security, Tools and Locations. To schedule a new Scheduled Meeting room, complete these tabs as follows however **DO NOT CLICK ON THE SAVE BUTTON.** The save button is used **ONLY** after you have completed all five tabs of the meeting tool.

a. **Essentials:**

- (a) Select the **Meeting Type**, normally Collaboration will suffice however Presentation modes are available.
- (b) **Enter 'Meeting name'**. Enter a name for the SM room. You can use any characters in the meeting name, including letters, numbers, spaces, and symbols. Choose a name that identifies the purpose of the SM room such as HiCom, MIO, Tac Coord.

Figure 35 - Setting Meeting Details

- (c) Change the **Moderator** as required.
- (d) **Schedule** either the time the SM will start and it's duration using the 'Schedule' function, or if the meeting is to start immediately after it is configured, ensure that '**Start Now**' is selected via the radio button.
- (e) The SM can be recorded for replay at a later date if required.

b. **Files**

- (a) This feature allows the sharing or presentation of files on the 'Whiteboard' in an SM room. Any PowerPoint presentations, images or documents expected to be used during the meeting should be load using

this tab. It is not possible to add/transfer files once an SM has started. Determine the files required and upload using the “**Attach a File**” button.

- (b) Enter a detailed description of the SM room if required.

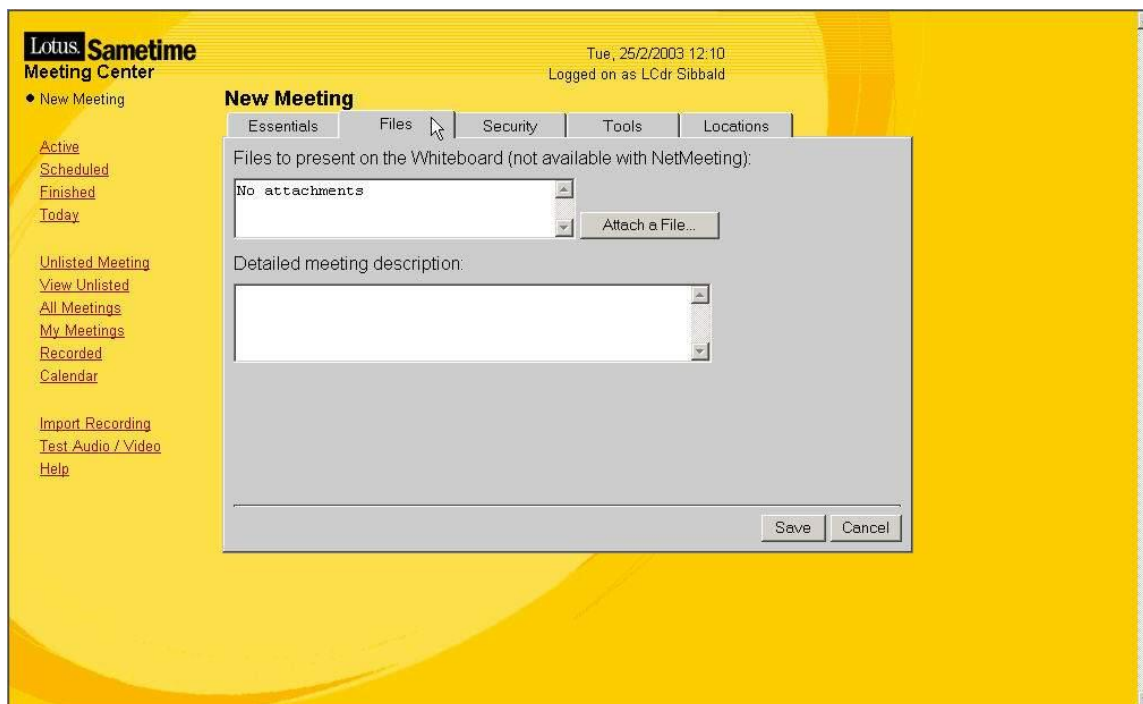
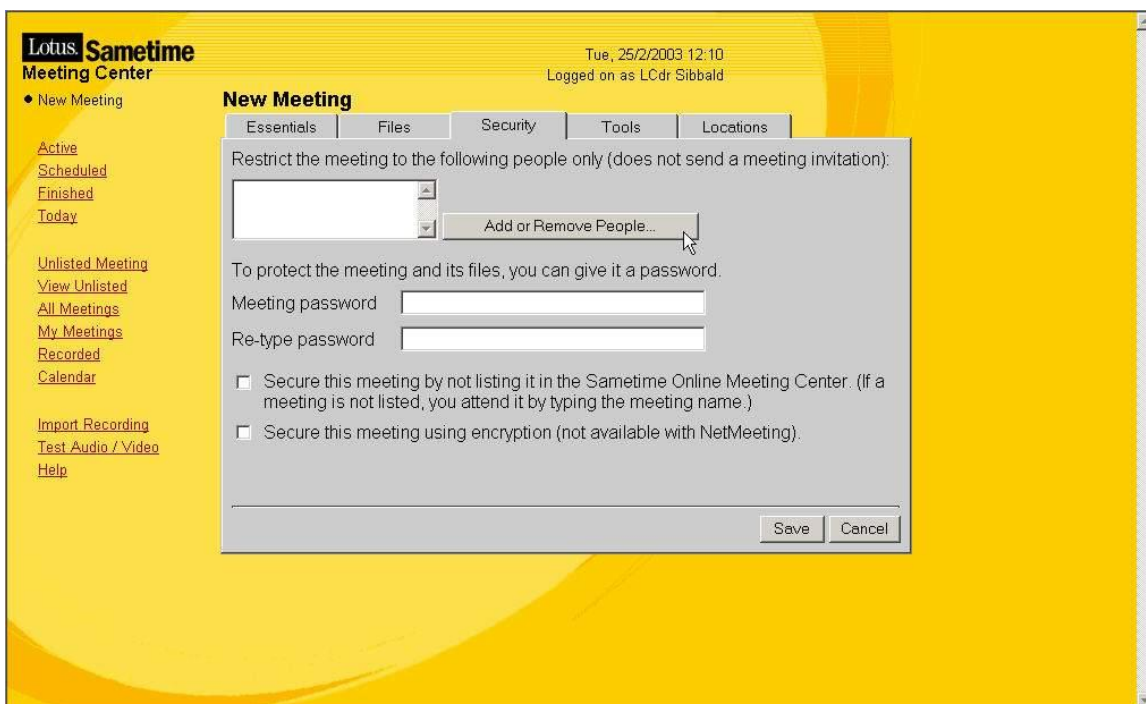


Figure 36 - Attaching Files for a Meeting

c. Security

- (a) Access to a SM Chat can be controlled using the Security Tab. The SM can be restricted to either a specified group of users or by password. A password may be added to a SM ensuring that only those users who have been provided the password are able to log in.
- (b) Additionally, a SM may also be 'Unlisted', so that it will not show up as an 'Active', 'Scheduled' or 'Finished' meeting in the Sametime Meeting Centre.
- (c) The encryption option will encrypt the meeting at 128bits.

**Figure 37 - Setting a Meeting Password**

d. **Tools**

- (d) This area allows the scheduler to select the tools that are required to be used in the SM room.
- (e) The default is 'all available tools' however due to bandwidth restrictions when conducting SM chat with ships over MTWAN, consideration should be given to deselecting most of the tools. The '**Meeting Room Chat**' is required and if there is a requirement to share files or to use the whiteboard, ensure '**Whiteboard**' is also selected and the necessary files have been loaded.

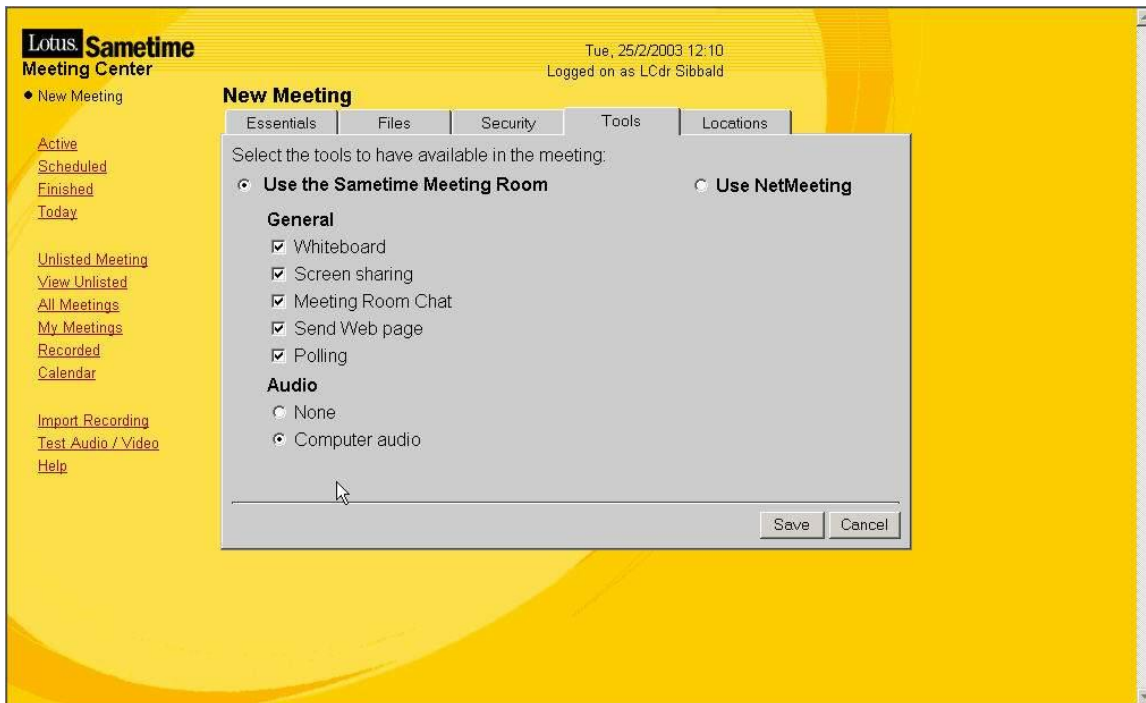


Figure 38 - Adding the Meeting Tools

(f) Unless needed, ensure 'Audio' is selected as 'None'.

e. **Locations**

(g) Ensure that both 'People are attending using a modem' and 'People are attending from internal Sametime servers' checkboxes are selected.

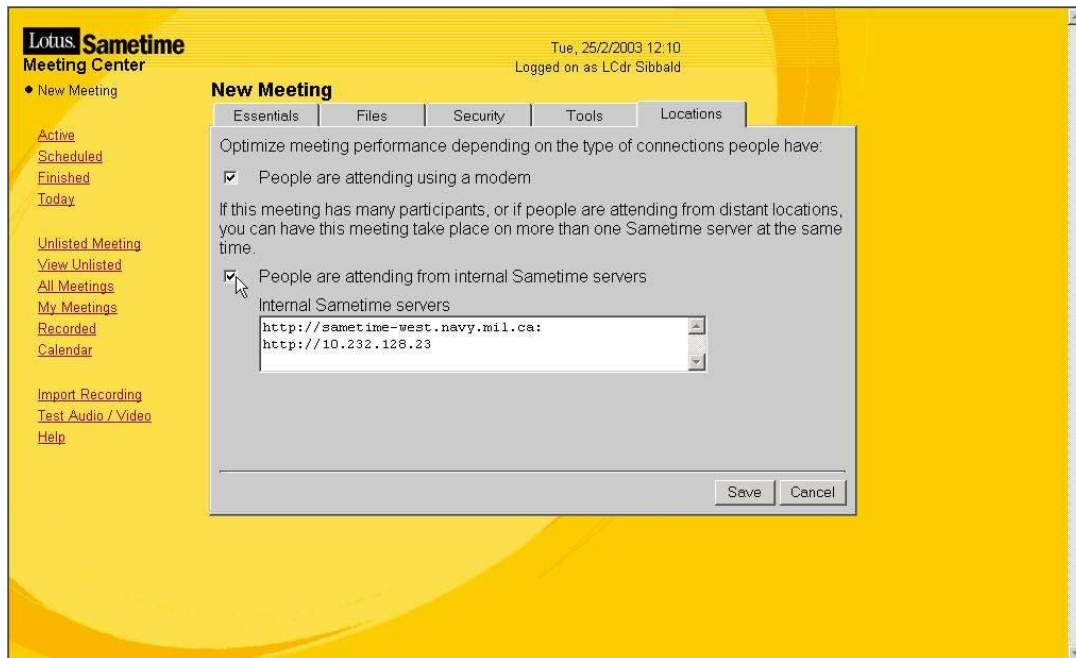


Figure 39 - Optimize Meeting Performance

41. Select the 'Save' button to save your meeting.
42. A summary page will appear, showing the details of scheduled meeting.

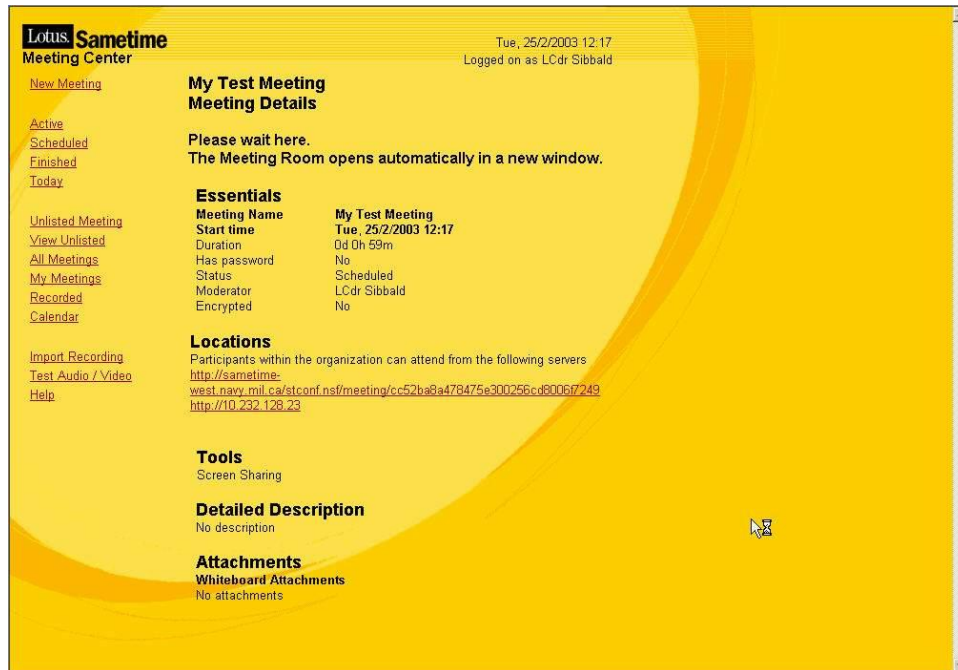


Figure 40 - Meeting Summary

43. If the 'Start Now' option was selected, the meeting will open automatically.

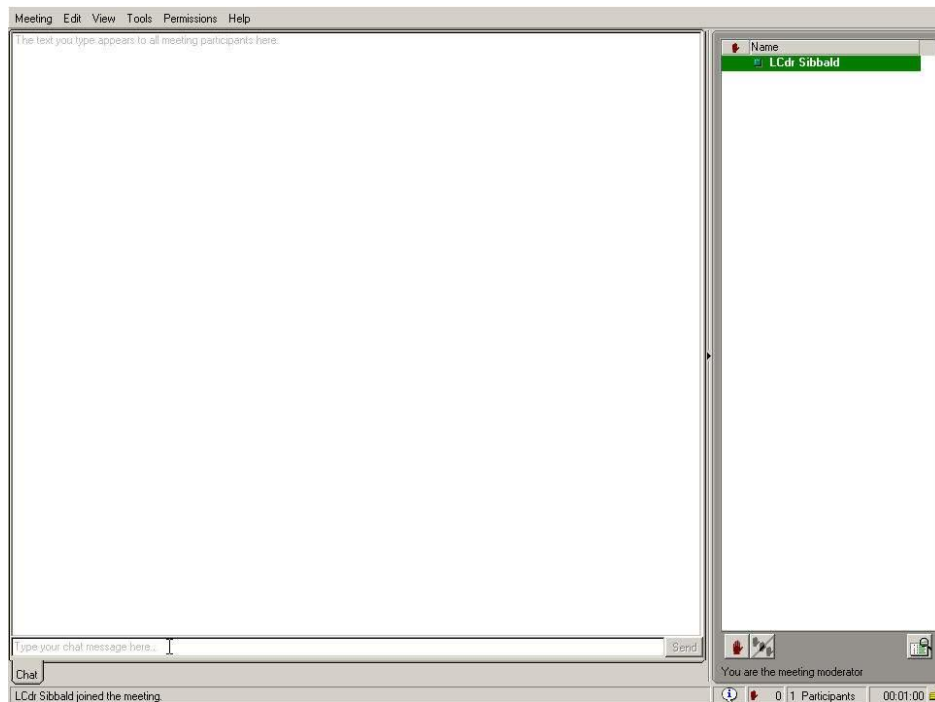


Figure 41 - Scheduled Meeting Room

ATTENDING A SCHEDULED MEETING (SM) ROOM

44. Unlike an IM room, users do not need to be 'invited' into a SM room in order to participate. This is because the meeting room remains available for use, even when there are no active participants. The SM room will remain active until the scheduled meeting duration time is met or the SM room is 'Ended' by the moderator.

45. The easiest way to join a SM Room is through the Sametime Meeting Centre in the web browser:

- a. Click on '**Attend a Meeting**' in the Sametime Meeting Centre.

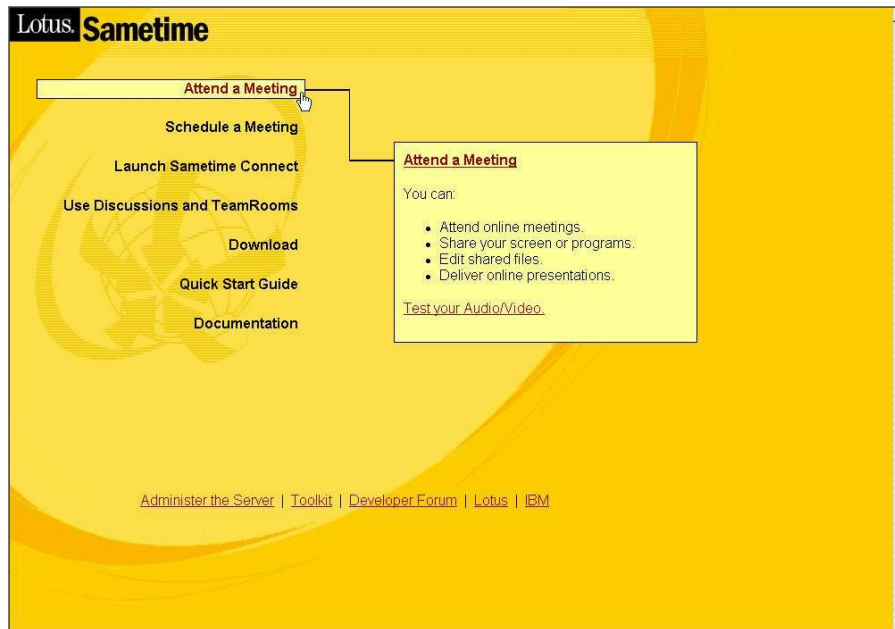


Figure 42 - Attending a Scheduled Meeting

- b. This will open the '**Active Meetings**' window. Ensure the user is logged onto Sametime.

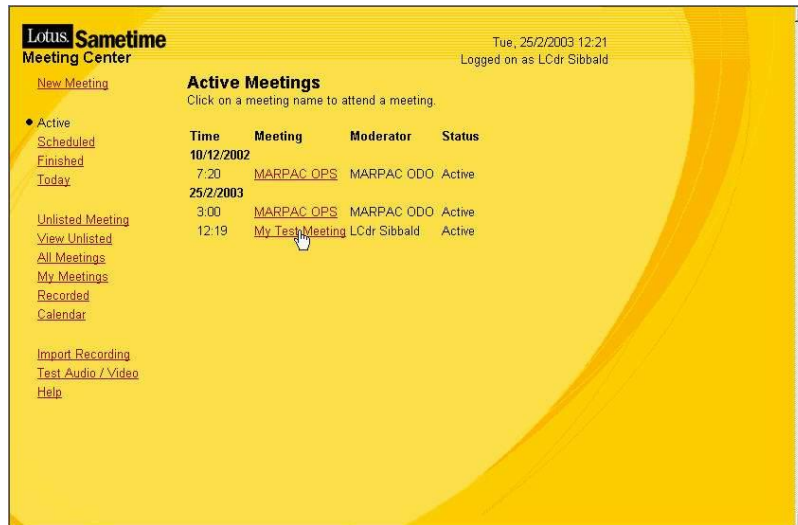


Figure 43 - Selecting the Scheduled Meeting

- c. Select the meeting that it is desired to attend. In this example the meeting is called 'My Test Meeting'.
- d. The SM room will open.

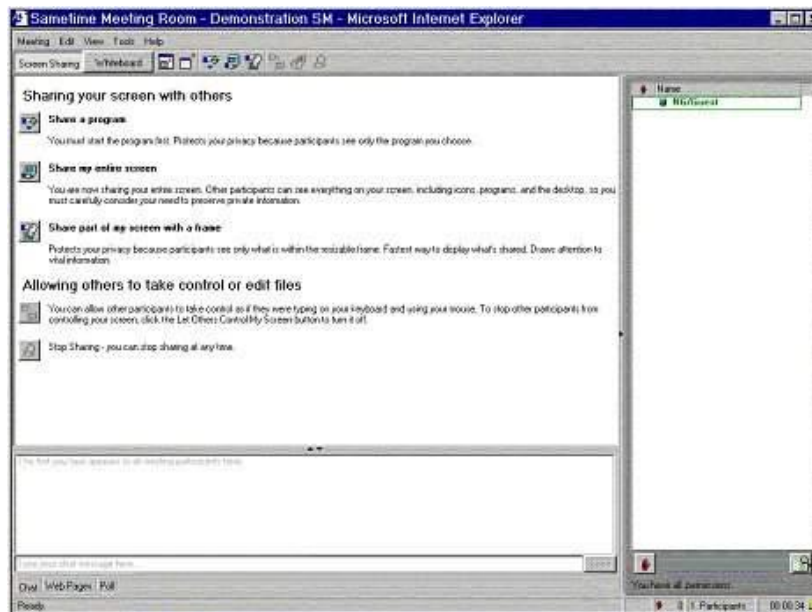


Figure 44 - Scheduled Meeting Room

ENDING AN SM CHAT

46. The meeting moderator has the option of ending the meeting prior to the scheduled end time by clicking on '**End Meeting**' in the '**Meeting Details**' page.

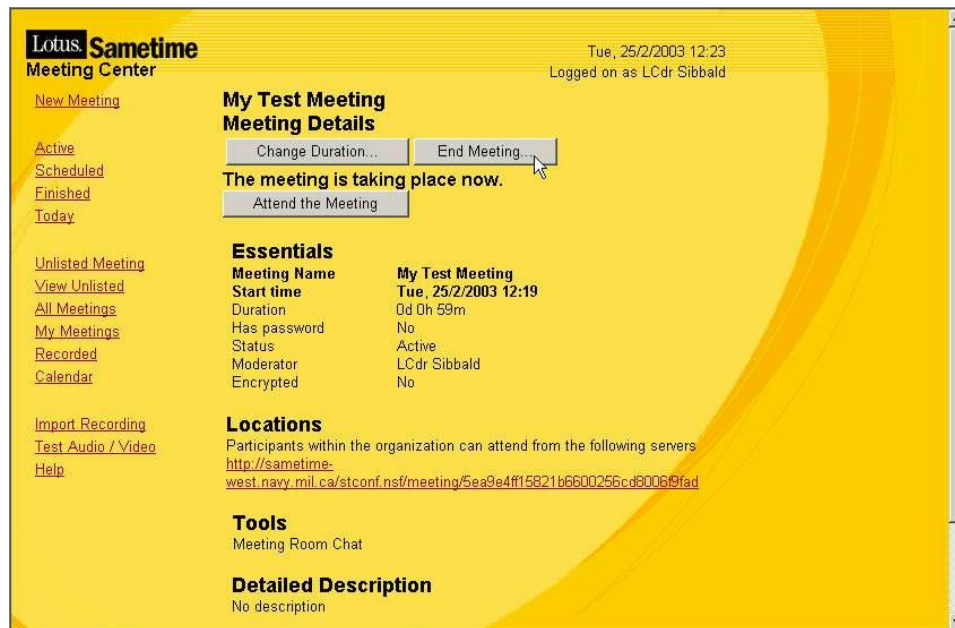


Figure 45 - Ending a Scheduled Meeting

- a. A 'confirmation' window will 'pop-up'. Select OK, in order to confirm the ending of a meeting.



- b. A confirmation page will appear, confirming that you have ended the meeting.

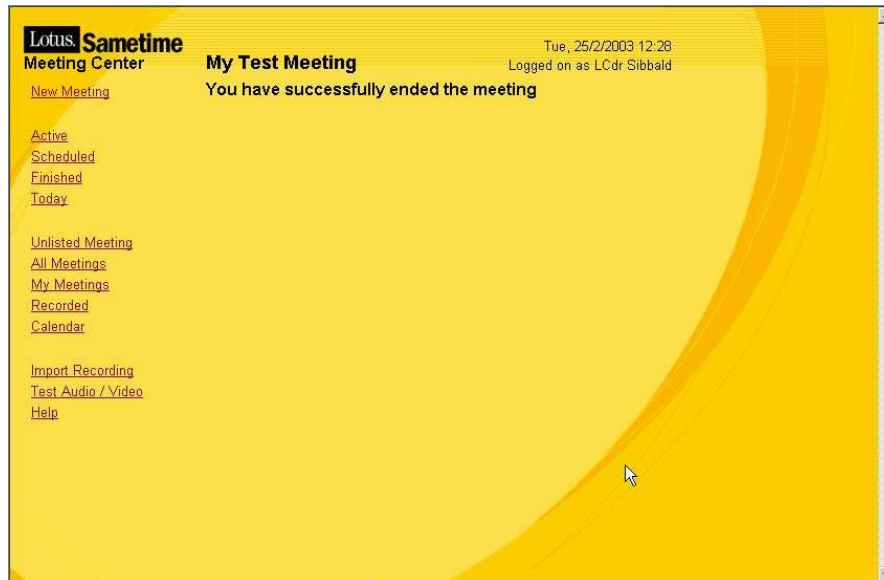
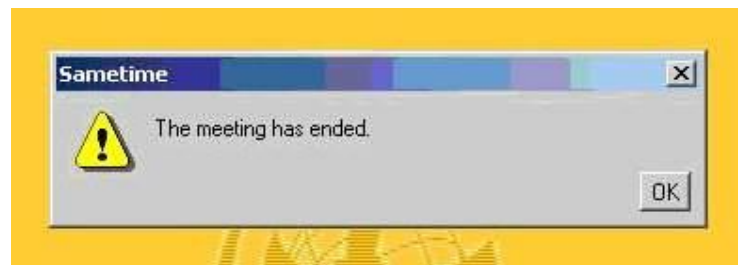


Figure 46 - Completed Meeting

- c. Users still in the meeting room when the moderator forces it's closure will see the dialogue box.



ADDITIONAL INFORMATION

47. Lotus Sametime has many advanced features that are not described in this basic user guide. In order to find out more information about Sametime and advanced collaboration tools, use the online guidebooks (Quick Start Guide and Documentation) that are found in the Sametime Meeting Centre.

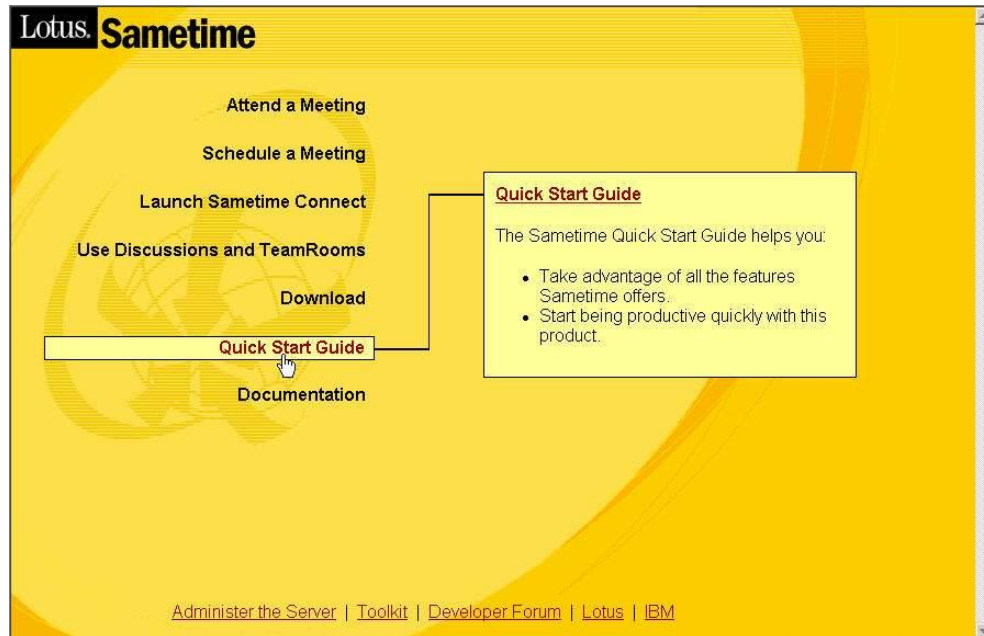


Figure 47 - Quick Start Guide

PERSISTENT CHAT

INTRODUCTION

1. The Instant Persistent War Room (IPWaR) application provides a number of private and persistent chat and file exchange collaboration rooms using the installed Sametime collaboration network. IPWaR, also referred to as Persistent Chat (PChat), is installed on the Sametime server and is accessed via a web browser using Domino/Sametime names and passwords for authentication. In addition to providing a private room for information exchange, IPWaR provides a number of additional enhancements for the user, including:
 - a. Retrieval of up to 96 hours of chat history within the room (persistence)
 - b. Automatic time stamping of all text chat entries
 - c. Persistent note and file storage area within each room for rapid dissemination of information for room participants only
 - d. User-tailorable alerts for each chat room
 - e. Individual chat rooms can be protected via unique passwords and/or restricted to specific authenticated users
2. Depending on the network chat configuration, access to IPWaR is normally via a Domino or Sametime server located onboard a ship at sea or through a shore based Sametime server over a WAN connection. The OPTASK Net and/or system administrator will provide the Login URL (or Web address).
3. Browsing to the appropriate URL will present the IPWaR's Login screen. However, if the particular IPWaR application allows anonymous access or the user is already logged in, a dialog box listing the available rooms (Figure 48) will appear:

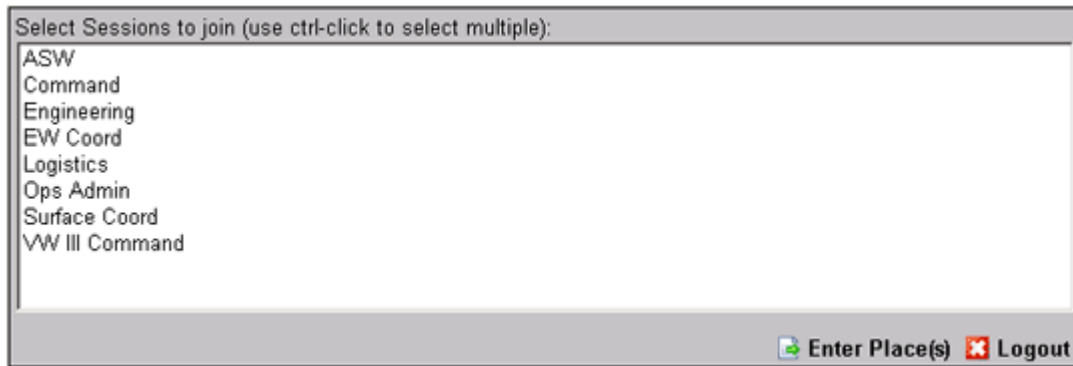


Figure 48 - Available Rooms

4. The desired rooms may be selected from this dialog box. Multiple Rooms can be selected using a combination of a **left mouse click** while holding down the “**Ctrl**” key. As well, by using a combination of a **left mouse click** while holding down the “**Shift**” key, all Rooms can be selected. When the desired rooms have been selected, **click** the option “**Enter Place(s)**”.
5. The main IPWaR screen will appear (Figure 49).

IPWAR’S WORK AREA

6. The IPWaR Work Area consists of a number of important areas. These areas include:
 - a. Room Tabs – The rooms selected in the previous screen are each represented by a tab. Clicking on a tab for a room will take the user into the selected room.
 - b. People within the Room frame – It displays the users currently in the active room.
 - c. Users Buddy list - Displays the user’s Sametime Buddy list.
 - d. Chat History - Displays chat that was recorded prior to the user entering the room and the chat since the user entered. All chat is automatically time-stamped by the application.
 - e. Text Entry Area - Text can be entered using the keyboard or “cut” from another application, and “pasted” into the text entry area. Text is sent using either the “Enter” key or the “Send” button.
 - f. Status Settings - A user can change their status displayed to other users by selecting one of the three Status settings:

- (h) ACTIVE - Represented by a green icon;
 - (i) AWAY - Represented by a yellow icon; and,
 - (j) DO NOT DISTURB – Represented by a red “do not enter” sign.
- g. Activity Tabs - Contains information specific to each Room. The Activity tabs consists of five (5) tabs (buttons):
- (k) ALERTS - Displays individualized customized programmed alerts;
 - (l) FILES - Displays shared files;
 - (m) NOTES - Displays shared text notes;
 - (n) BOOKMARKS - Displays shared URLs (Web links); and,
 - (o) SEARCH - Displays the Search window for past chats, Files, Notes and/or Bookmarks.

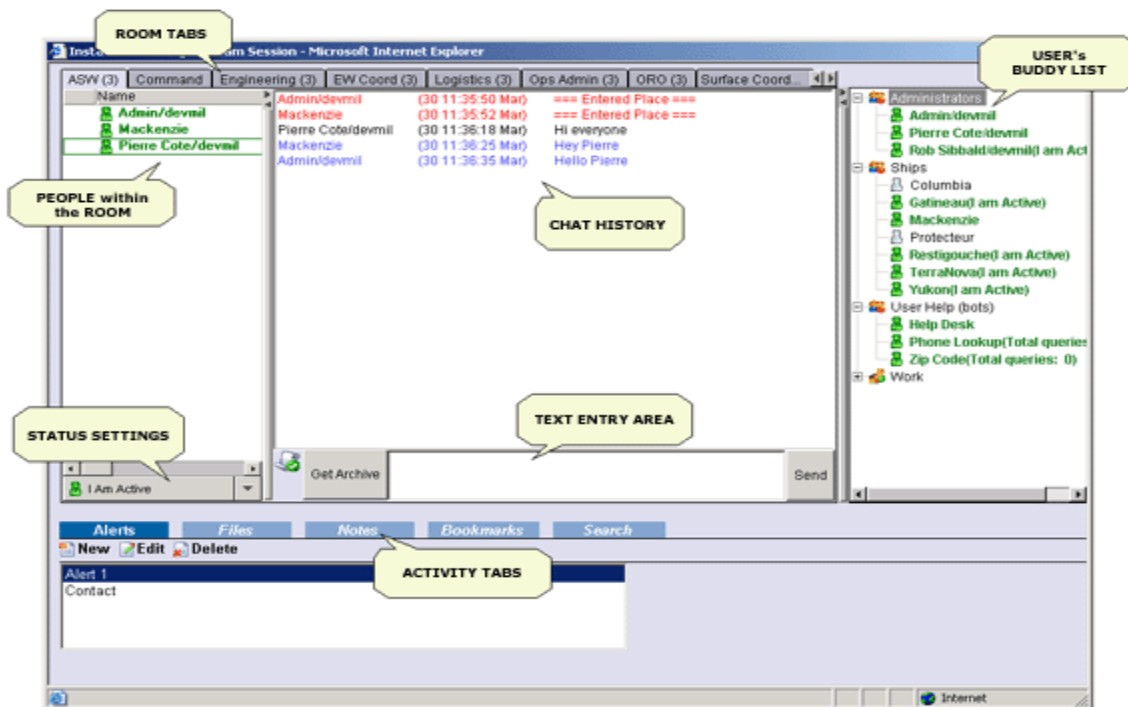


Figure 49 - Main IPWar Screen

ROOM TABS

7. Room Tabs represent each room that the user entered (selected). The name of the room is shown on the tab itself. The number in parenthesis (to the right of the Room name) shows the total number of people in the room. The active tab is displayed in a different color

and in a higher plane to other tabs. The following screenshot shows “Engineering” is the active Room.



Figure 50 - Room Tabs

8. While a Room is selected (“Engineering”), the user is still active in the other rooms. However, if chat is received in another room (“ASW”), the other room will change color to indicate that text was received as can be seen here for the “ASW” room.



Figure 51 - Receiving Text in Non-Active Room

9. If a user has a custom “Alert” on a room (explained in more detail below), and the option to “Flash Window” was selected, then the tab will ‘flash’ when activated. This helps to ‘catch the eye’ of the user who set the alert.

CLOSING AN ACTIVE ROOM

10. A user can close a room by using the **right mouse button** on the tab, and selecting Close (as shown below).



Figure 52 - Closing the Active Room

PASSWORD PROTECTED ROOMS

11. Some rooms can be password protected. When entering a password-protected room, the user will be presented with a dialog screen asking for the password as can be seen here:

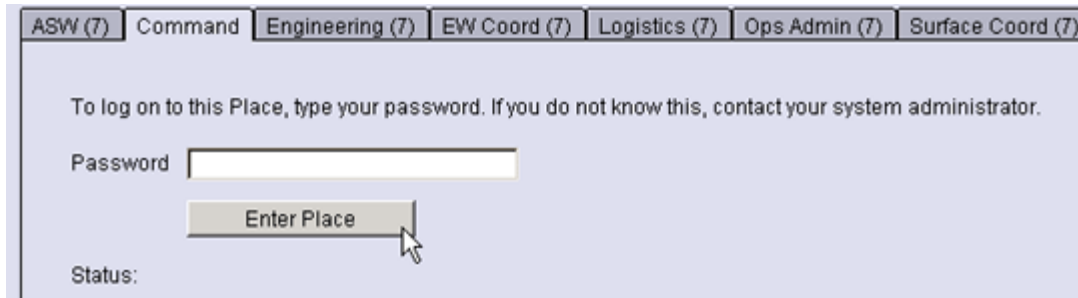


Figure 53 - Password Protected Rooms

12. If it is necessary to refresh the Activity tabs for your active room, **click** on the active room tab with the **left mouse button**.

PEOPLE WITHIN THE ROOM FRAME

13. The “People within the Room” frame displays the active users in a room. This list of users can vary from room to room and is also dynamic. This means that when a user enters or leaves a room, their name will either appear or be removed automatically from the “People within the Room” list and the “participant counter” on the Room tab (the number in parenthesis) will be amended accordingly. The “People within the Room” frame also displays if a user is typing a message with a small icon (keyboard and blue arrow) as shown against HMCS Mackenzie below.

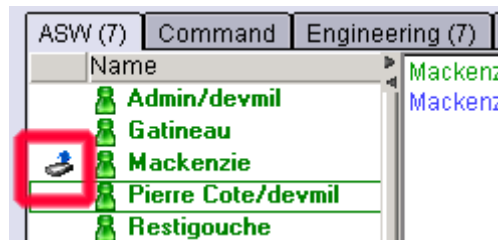


Figure 54 - People within the Room

USERS BUDDY LIST FRAME

14. The Users Buddy list frame displays the logged-in user’s Sametime Buddy list that is stored on their Home Sametime server. Using the **right mouse button** on the Buddy list, a user can choose to show online users only. This setting is saved across all sessions.
15. In the frames for the “Buddy list” and “People within the Room”, on the frame separator are two triangular buttons (circled). One will collapse the frame and the other will expand it out.

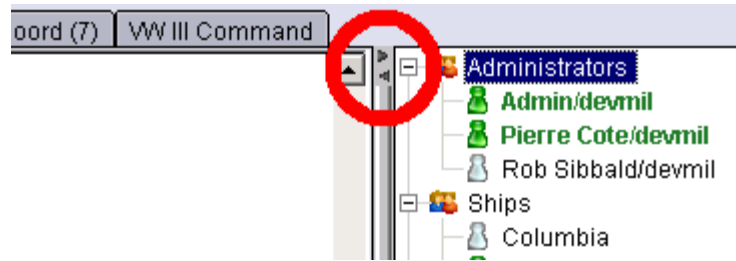


Figure 55 - Collapsing/Expanding Lists

16. The frame can also be sized by dragging the side of the frame with the **left mouse button** depressed.

Note: If the user has no Home server specified, the Buddy list is retrieved from the Sametime server the user logged into at the beginning the session.

SENDING A FILE

17. If approved, users are able to use their “Buddy list” or the “People within the Room” frames to send files directly to other users. This option is available by selecting a recipient using the **right mouse button** menu.

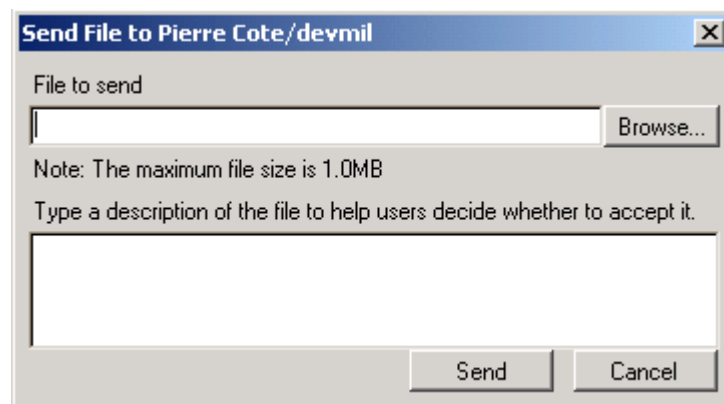


Figure 56 - Sending a File

Notes Files sent through the “Buddy list” File Transfer are neither stored in the room nor available to other users.

18. The “Buddy list” within IPWaR is Read-Only. Users cannot be added or removed through the IPWaR interface. This can only be done directly at the Sametime Connect client.

CHAT HISTORY AREA

19. The Chat History area is where prior chat history is displayed. It also displays chat that was recorded prior to the user entering the room as well as the chat since the user entered. The details for each chat line that are displayed are:

- a. The person who sent the text;

3C-5

UNCLASSIFIED

Original
(Reverse Blank)

- b. The time the text was sent; and,
 - c. The text that was actually sent.
20. The Chat History area text also automatically records and displays specific room activity including: when people enter and/or leave the room and the posting of a new File, Note or Bookmark.
21. Historical text can be retrieved at any time by selecting the “Get Archive” button; found just to the left of the Text Entry Area. When the user retrieves this data it is displayed only within the user’s Chat History Area. A fixed length of time for archiving chat can be set for each specific room when the collaboration room is first created. It will be this selected time period that will be retrieved and displayed whenever the ‘Get Archive’ button is used. IPWaR can be configured so that the archived text is automatically retrieved and displayed upon initial entry into the collaboration room.



Figure 57 - Retrieving Archives

22. The text being displayed can be shown in different colors. Most colors are defined by system administrators and are used to differentiate the following items:
- a. Chat History,
 - b. Live Chat,
 - c. People entering and leaving the room,
 - d. Activity Posting, and
 - e. The text that matches an Alert - This color is defined by the user who actually created the alert.
23. A user can select text in the chat history area and copy it to the clipboard using the **right mouse button** menu and selecting “Copy”.

TEXT ENTRY AREA

24. The Text Entry Area is where a user can enter text to send to other people within the room. When a user enters text, the text is sent by either pressing the “Enter” key or selecting “Send” with the mouse.
25. The user can paste text into the text entry area by using the **right mouse button** menu and selecting “Paste”.

26. To the left of the Text Entry area is a small indicator displaying if the chat is being archived as shown here (green checkmark):



Figure 58 - Text Entry

27. If the text is not being archived, a small red cross (“X”) is displayed in place of the checkmark on a green background. The user can also click on the icon itself to see the status of the “Archiver”.

STATUS SETTINGS

28. The Status Settings area of IPWaR allows a user to change their Status settings. A user can set their Status to one of three states. These states are:

- I Am Active - Represented by a green icon;
- I Am Away - Represented by a yellow icon; and,
- Do Not Disturb Me - Represented by a red “do not enter” sign.

29. To set their status, a user clicks on the “drop down arrow” as shown here:

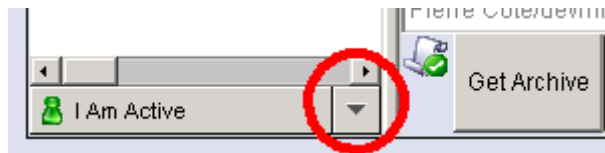


Figure 59 – Status Indicator

- This will display a dialog where the user can enter their Status description. This is displayed to other users when they “hover” the mouse over a person’s name in the “People within the Room” frame or their regular Sametime Connect client.
- By selecting the button to the left of the “drop down arrow” (as shown below), the user can change their Status description without changing their Status state. However, it is recommended that the **defaults be utilized to avoid confusion** (such as the three states indicated above).



Figure 60 - Changing the Status

ACTIVITY TABS

30. The Activity tabs are where additional information can be tracked and shared with fellow users in a room. The contents of the Activity Tabs are **unique** to each room. There are five activity tabs: Alerts, Files, Notes, Bookmarks and Search.



Figure 61 - Activity Tabs

31. By clicking on an Activity tab, the application will display the related information for the selected room. The Activity Tabs area of the collaboration room can be configured to operate in a 'replicated' environment mode.

32. When configured for a 'replicated' environment all information in this area must be 'replicated' to other ships/shore units before remote users can access the information. Chat, buddy lists, participant awareness, etc. remain "real time" and are not affected by replication. More details and impact assessments for different IPWaR network configurations can be found later in this document.

ALERTS

33. Alerts are personal to each user. Multiple alerts can be entered into rooms so that if certain criteria are met for incoming text, the user can be notified. Alert matching is performed on incoming text (chat).

CREATING AN ALERT

34. To create a new alert, the user performs the following steps:

- a. Click on the "Alerts" Activity tab button. Then, select the "New" button as indicated here:

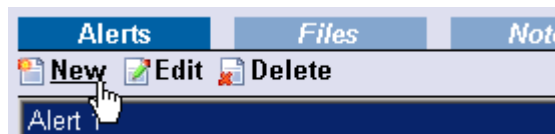


Figure 62 - New Alert

- b. The user is presented with the "Create new alert" dialog box:

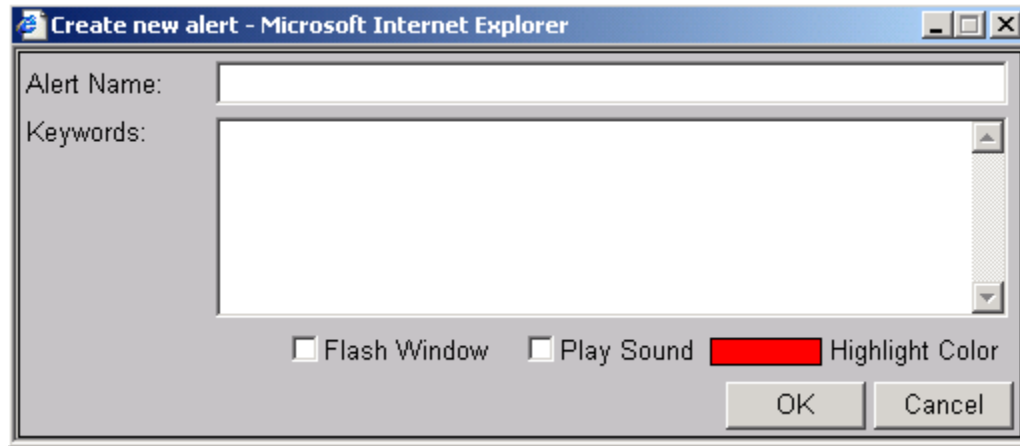


Figure 63 - Create New Alert Dialog Box

- c. Enter a name used to represent the alert. Use a descriptive name that easily identified each alert.
- d. Enter the keyword(s) desired to match for the alert. Keywords are the power of "Alerts". Keywords are how the system knows when to notify the user that one of the predefined alerts matched incoming text. There are a number of search options that can be entered in the Keywords section and multiple searches for a single alert can be separated with a new line. See the section "Keyword Syntax" for the syntax of keywords.
- e. Choose "Flash Window" if it is desired that the Window be brought to the front or flash the Room tab if the alert is matched with incoming text. By selecting this option, if the IPWaR application window is in the background or minimized, the Window will come to the front and take focus. If the Window is already active and an alert is matched on a Room tab without focus, then the tab where the alert was met will flash.
- f. Choose "Play Sound" if it is desired that a sound be played when the alert keyword(s) is/are met. By selecting this option a sound notification will be played when the alert is matched.
- g. Choose a highlight color (by clicking on the red rectangle as demonstrated below). This color will be used to highlight the text in the Chat History frame.



Figure 64 - New Alert Color

- h. When the desired “Alert” has been entered, click the “OK” button.
- i. The Alert is now active for this particular Room.

Note: Alerts do not process the text the user SENDS, only the INCOMING text. As well, the Administrator can specify if alerts are processed on history text.

KEYWORD SYNTAX

35. There are a number of syntax options for searching for matching words within an IPWaR application “Alert”. Users familiar with DOS type searching will be comfortable with IPWaR’s “Alerts” syntax. The various keyword syntaxes are:

TYPE	EXAMPLE	RESULTS
Word	Clock	Finds the complete word “clock”. A word search is not case sensitive. clock, clocks, cLoCks and ClOcK are all positive matches.
Partial Word	*ock	Finds a word that ends with "ock": block, sock, dock and clock are all positive matches.
	clo*	Finds a word that begins with "clo": cloth, clot, clod and clown would all be positive matches.

TYPE	EXAMPLE	RESULTS
	oc	Finds a word that contains “oc”: clock, rock, Hock are positive matches.
Wild Cards	?lock	Finds a word preceded by a wildcard character. So ?lock would match clock and block, but not clocks or blocks.
	cloc?	Finds a word followed by a wildcard letter. cloc? would match clock and clocks, but not aclock, bclock or dclock.
Exact Match	“ABC”	Finds an exact match in both case and length. “ABC” would match ABC, but not aBc, AbC, ABCDEF, or BABC.

Table 2 - Keyword Syntax

FILES

36. The “Files” Activity tab allows users to upload and share files with other people. Unlike the File Transfer option in the Buddy list covered above, files shared through the “Activity Tabs – Files” can be seen by all users, and accessed at a later time.

37. The “Files” tab displays important information about attached files including the file name, the file description and its size.

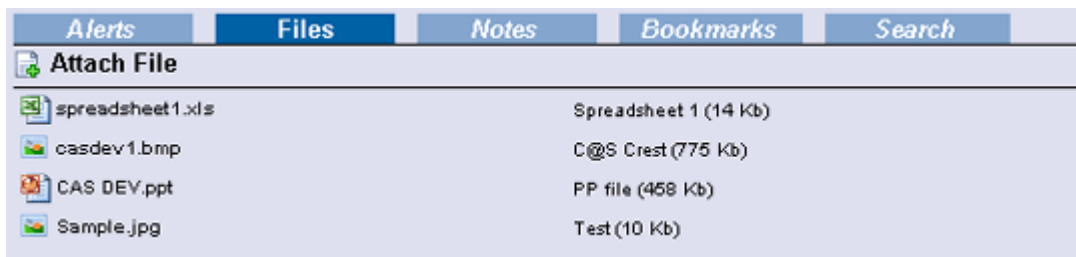


Figure 65 - Files Tab

ATTACHING A FILE

38. To attach a file to the room, click on the button “Attach File” (with the “Files” tab selected). Enter a description for the file, and “Browse” to the file location. When the file is found, click “Upload”.

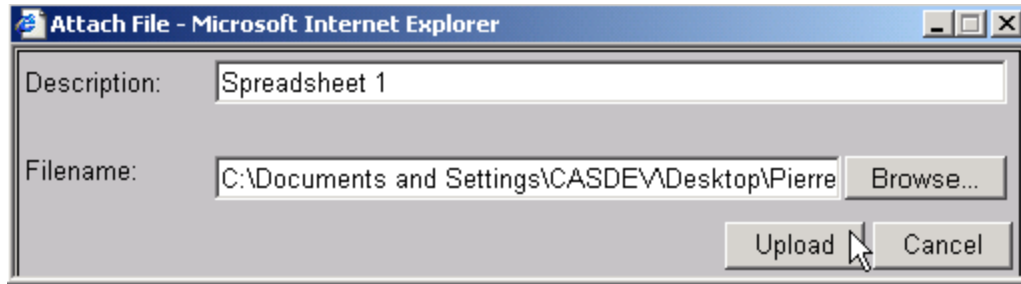


Figure 66 - Attaching a File

39. When the file has completed uploading, a notification is sent to the other users in the room and the “Files” Activity tab is refreshed to show the attached file.

NOTES

40. The “Notes” Activity tab allows for sharing simple notes between users within an IPWaR room.

CREATING A NOTE

41. To create a “Note” within the room, select the button “New Note” (having clicked on the “Notes” tab). Then, type a description for the note and within the “Note” field enter the plain text note. Alternatively basic HTML tags such as (bold), <I> (italic), <U> (underline), (unordered list), etc. can be entered to create smart looking “Notes”. For example this simple HTML “Note”:

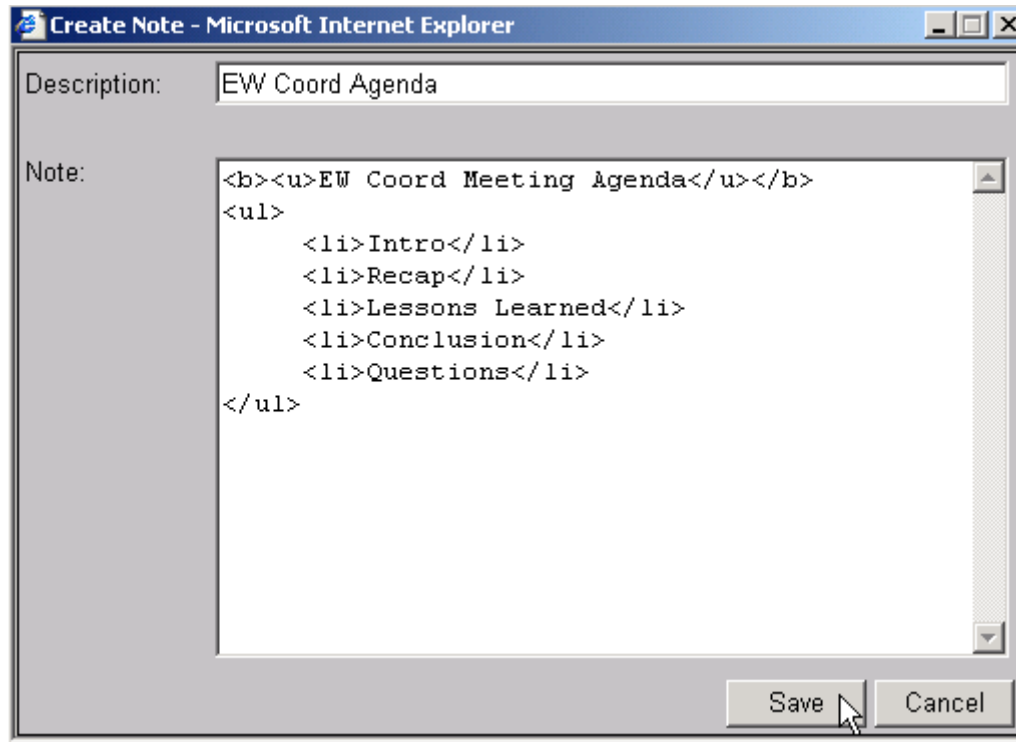


Figure 67 - Creating a Note

42. The HTML tags used above looks like the following when opened by users once the note is "Saved":

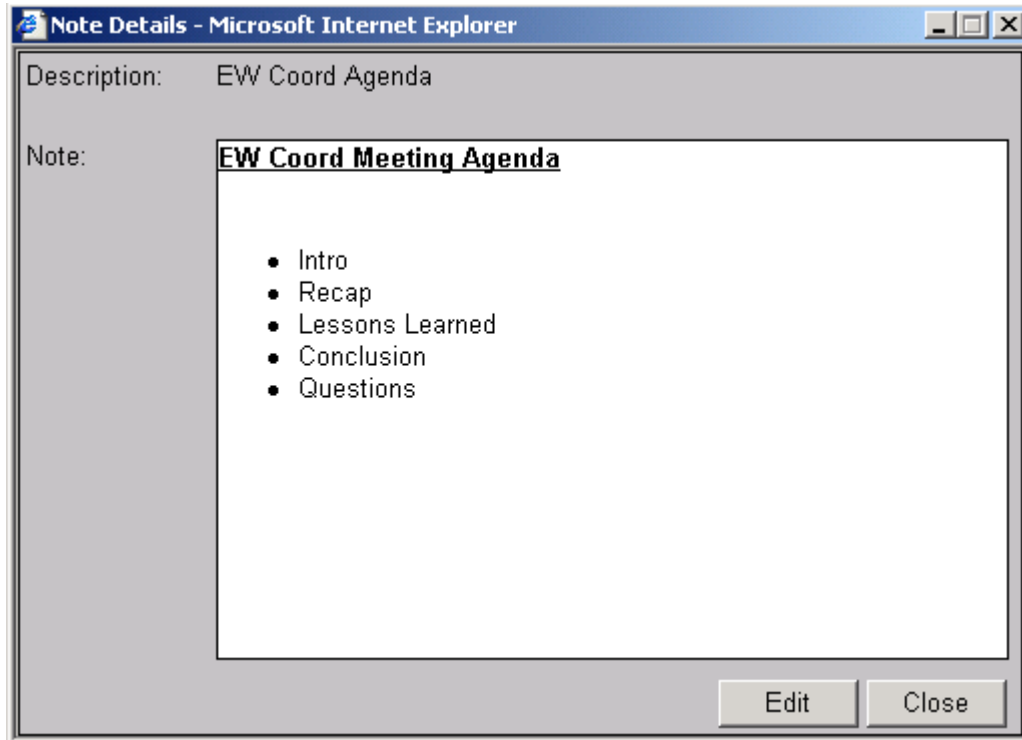


Figure 68 - Note Details

43. This figure also illustrates how the creator of a “Note” can change it at any time by selecting the “Edit” button.

BOOKMARKS

44. The “Bookmarks” Activity tab allows users to share Internet Bookmarks (similar to Favorites in Microsoft’s Internet Explorer) with other users in a Room. By selecting a bookmark entry from the Activity Tab, a new browser window will be opened at the shared location.

CREATING A BOOKMARK

45. To create a “Bookmark”, select the “New Bookmark” button (while within the “Bookmarks” Activity tab). Then, type a description for the bookmark, enter the URL Link (Web address) location and click “Save”.

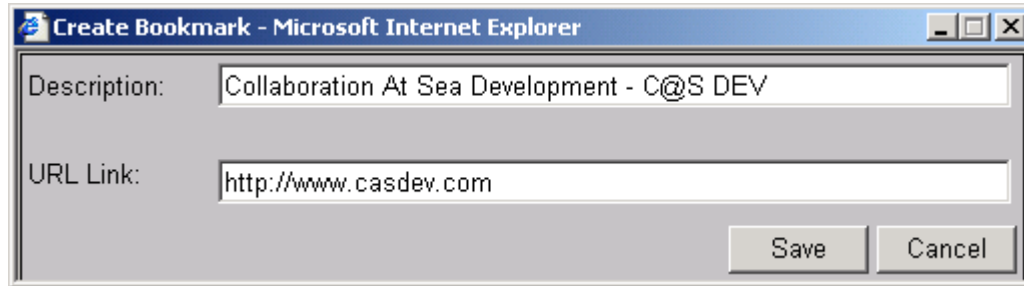


Figure 69 - Creating a Bookmark

SEARCH

46. The “Search” Activity Tab gives the user quick access to search archived Chat (text), Files, Notes and Bookmarks for specific content.

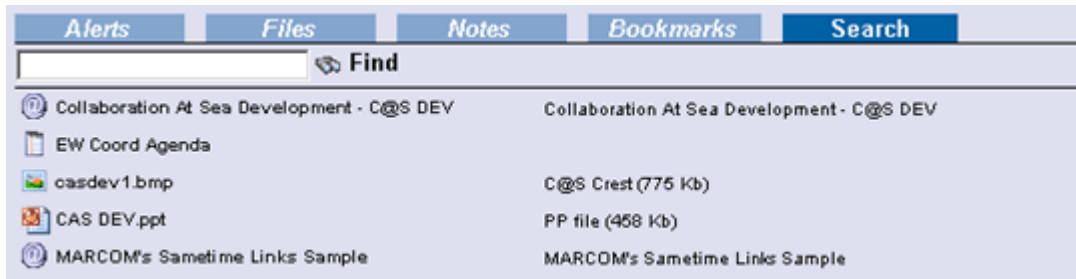


Figure 70 - Search

PERFORMING A SEARCH

47. To perform a search, type the words (or keywords) being searched for, separated by a space and **click** on the “Find” button. The IPWaR application will then return any matching Chat, Files, Notes and/or Bookmarks that contain the entered words/keywords.

CHAPTER 4**WEB SERVICES****INTRODUCTION**

401. The key to Web Services is the availability of authoritative data and the ability to reuse it. An IP network, while providing connectivity, in itself does not guarantee the ability to seamlessly share data. This is because IP-enabled applications often use application-specific mechanisms to format and transmit data over networks. Web Services utilize a 'web browser' to provide a common User Interface (UI) application between the data and the user. This negates the requirement for individual workstations to be loaded with numerous unique applications prior to being able to access and share information.

COLLABORATION

402. The basic goal of collaboration is to consolidate tactical, operational, and selected administrative information regarding the status of, and planning for a force in one central location easily accessible to the user community. Web sites serve as a central repository for a wide range of operational information and reports. They work in conjunction with other communication tools (such as e-mail, record message traffic, real-time computer-based chat, and voice and video communication) to enhance overall shared awareness, speed of command, and collaborative planning and execution capabilities. In many cases, they can replace traditional means of communications with a more efficient, intuitive tool. Information that can be shared includes the following:

- a. Mission statement
- b. Course of Action
- c. Intelligence Summary
- d. Commander's Critical Information Requirements
- e. Commander's Intentions
- f. ROE Update
- g. Weather Summary
- h. Logistics
- i. CASREPs
- j. Fuel and Provisions
- k. Ammunition Status

- l. Order of Battle Matrices
- m. Policy guidance for intelligence collection strategy
- n. Various daily intelligence products
- o. Air Tasking Orders (ATOs)
- p. Operational Tasking (OPTASK) messages
- q. Maritime Interdiction Operations (MIO) Intelligence

COLLABORATION AT SEA (CAS)

403. Lotus Notes and Domino Server software suites are being used to support Collaboration at Sea (CaS) web services. These web sites are composed of document databases, with documents defined as any file. Templates integrate these databases and provide tailored views of the documents from within any standard web browser. These templates provide updated, comprehensive information vital to coalition operations. The system also contains a directory of users allowing rapid identification of personnel throughout the network. Any user needing web editing or authoring capability (or access to SameTime Chat services) must first establish a user account. Any user requiring a user account will need to follow the policy and procedures outlined in their national doctrine.

404. Shore authorities administer both shore and shipboard Domino servers. This relieves the war-fighter of many of the information technology issues, allowing them to concentrate on the mission and more effectively utilize the tactical information at hand. Transaction logging within Domino keeps track of the replication status. If communications (or connectivity) are lost for any reason, replication will cease. When network connectivity is re-established however, replication will recommence at the point at which it ceased, thus limiting expensive communication and satellite resources. Replication schedules are determined by the Commander and promulgated in the OPTASK IM. These schedules would normally require replication to automatically occur on a fixed schedule, generally 30 minutes after the completion of the last replication cycle.

405. Authorized personnel have the ability to view web site data via any standard web browser. Users with the appropriate permissions have the ability to post items directly to web sites, without the intervention of a Webmaster. This posting can be accomplished via any standard web browser and allows the content provider to focus on the quality of the content rather than the display and posting mechanics. Knowledge can be shared without having to traverse the chain of command. It is important to note that these sites are not intended for the conduct of real-time operations, conduit of immediate action items, or the issue of orders or commands (which generally require real-time interaction or other modes of communication). Classified content added to these web sites is controlled by individual national policies.

406. Replication is the key to the use of a web site as an information tool for forces with limited bandwidth. Replication requires a copy of the entire web site to be resident upon servers located at each site. Users at the local site then access the information via that site's local area network (LAN). When a change is made locally to the web site (i.e., new information is posted), the change is replicated from the location where it was made, and communicated over the WAN to a master server location. The master server then transfers that change to the replicas of the web site at other local sites via the WAN.

407. Annex A to this Chapter provides the details of Collaboration at Sea (CaS) web features, a Domino based system developed for the CENTRIXS networks that takes advantage of Domino's replication ability. Care must be taken to ensure that the browser being utilized on the network supports the required Web Service applications.

WEB POLICY

408. Development of web pages requires time and skill. The content of a web page will also invariably require a good understanding of the CONOPS for the exercise, operation or mission. A command or technical support staff member will generally undertake this activity. ACP 200 Ch 8 provides guidance for web service and content.

409. A significant advantage of using a web page to make information available is the speed with which the information can be posted, the efficient use of bandwidth, and the central management and hosting of information. Units will 'pull' information from the site at the most appropriate time to the command.

410. Web content and authoring rights will vary depending on the exercise, operation or mission. The tactical commander must consider what information should be available and to whom, and who is authorized to provide information to the web page.

COLLABORATION AT SEA

INTRODUCTION

1. This Annex provides an overview of the Lotus Domino web features and applies to Collaboration at Sea (CaS), a Lotus Domino based system developed for the CENTRIXS networks that takes advantage of Domino's replication ability. Care must be taken to ensure that the browser being utilized on the network supports the required Web Service applications.

ACCOUNT ESTABLISHMENT/REGISTRATION

2. All users with the ability to login to the network can view their respective CAS sites however an account is required for those users who need edit capabilities for a CAS site. Edit capabilities can include the ability to post data or modify the existing Web site structure.

CAS REGISTRATION

3. Depending upon the MWTAN or CENTRIXS domain in use, individuals request new user accounts, and update account information, through the user registration site. Accounts give users access to Sametime Chat as well as site editor or administrator privileges. CAS administrators also use this site to manage individual user accounts and access levels.

4. The User Registration database resides at the NOC, and not on the local site servers. Therefore new user's account information must replicate from the CAS hub server to the local site server before new users can login and execute assigned privileges.

SELECTIVE REPLICATION

5. CaS features the ability for users on surface combatants and submarines to preview the data and select the documents that they want replicated to their ship/submarine. In each case, the user is presented with the option to mark the request as a "subscription" so that all updates are automatically replicated to them or to request the document on a one-time basis (would have to re-request if the document is updated).

ENHANCED SITE CUSTOMIZATION

6. CaS features full site customization by the Shipboard administrative team. The administrators can select from a number of preset options available to them or create sections of their own.

ONE-CLICK ACCESS TO LIBRARY FORMS TO POST

7. From the front page of the CAS 2.x site, the posting of a document into any library is one click to access the form to complete. This represents a two to four click reduction over prior versions of CAS. Administratively, this feature can be turned off.

ONE-CLICK ACCESS TO LIBRARIES TO BROWSE

8. From the front page of the CAS 2.x site, the accessing of a document into any library is one click to access the page with the document listing. This represents a two to three click reduction over prior versions of CAS. Administratively, this feature can be turned off.

ONE-CLICK ACCESS TO RECENTLY POSTED DOCUMENTS

9. From the front page of the CAS 2.x site, the accessing of new or updated documents is now a one click to select your time interval and see the display of documents. This functionality has been improved over prior versions and has now become standard in all of the CAS 2.x sites. Administratively, this feature can be turned off.

ABILITY TO CONFIGURE RECENT POST TIME INTERVALS

10. Shipboard administrators have full control over the time intervals that are displayed under recent posts. As mentioned above, this feature can also be turned off so it is not an option on the front page of the site.

SCAN SIZES OF RECENTLY POSTED DOCUMENTS

11. From the Recent posts view, you can also access a listing of documents by size thus allowing administrators to monitor the sizes of the documents posted to the CAS site.

ENHANCED INTEGRATION WITH STOPLIGHT

12. CAS 2.x builds upon the integration with the Stoplight application tool that was rolled out to the fleet in mid-2002. CAS 2.x features enhanced integration tools in every area of the site-allowing user to move links into Stoplight much easier.

POC AND CONTACT INFORMATION PER SITE SECTIONS

13. CAS 2.x features the ability to designate a POC for each section of the CAS site thus allowing users to contact the manager of the section with questions.

ENHANCED ABILITY TO ALLOW FOR FINE GRAIN ACCESS CONTROL

14. CAS 2.x architectural design will allow CAS administrators to set the access control on each area within the site. These access controls combined with the ability to register for certain sections (e.g., set library access to a specific group of approved individuals).

DOCUMENT LIBRARIES

15. Common look and feel - CAS 2.x library areas will have a common look and feel while allowing the administrator of the area to configure certain settings in accordance with the requests of the user (e.g., expanded or collapsed display).

16. Ability to control reader access - CAS 2.x library areas will have allow the poster of the document to specify if there are certain read restrictions on the document.

17. Ability to control Replication - CAS 2.x library areas will allow the poster to set certain restrictions on the replication of their documents.

18. No Distribution - Distribution of the document will be limited to the ship it was posted on and the NOCs.

19. Limited Distribution - Distribution of the document will be on a requested basis. Document will be replicated to the NOCs. All units designated as High-Bandwidth will receive the documents. All users on Low-Bandwidth ships will have the ability to request the document on a one-time or subscription basis.

- a. Distribute to all (*optional*) - Distribution of the document will be sent to all servers. This option is activated at the discretion of the shipboard administrator. This option is an override of the document distribution limitations.
- b. Folder or Tree views - Allows for the document listing display to be shown in the standard Domino hierarchy (blue triangles) or to be display via folder structure like Windows Explorer.

20. Library Configuration Options

- a. Pre-Define Categories - Allows a listing of categories to be predefined while also allowing user entered categories.
- b. Expand/Collapse settings - Allows for the library default to be set as Expanded or Collapsed on open. This is a feature that was requested for libraries that have a lower document count need to be opened as expanded and for libraries with higher document counts to appear as collapsed.
- c. Document History - Document history is maintained for each document with the shipboard administrator being allowed to set the number of updaters that appear in the list.
- d. Max Size Limitation for documents - Shipboard Administrator has the ability to designate a maximum size limitation for the library thus preventing the posting of attachments that exceed the Commander's OPTASK IM for CAS.

- e. Content Manager/Contact Data - The content manager's name and information can be added to the library so that users can contact them with questions.

FRONT PAGE OVERVIEW

21. This is an example of how the front page of a CAS 2.x site can be configured.

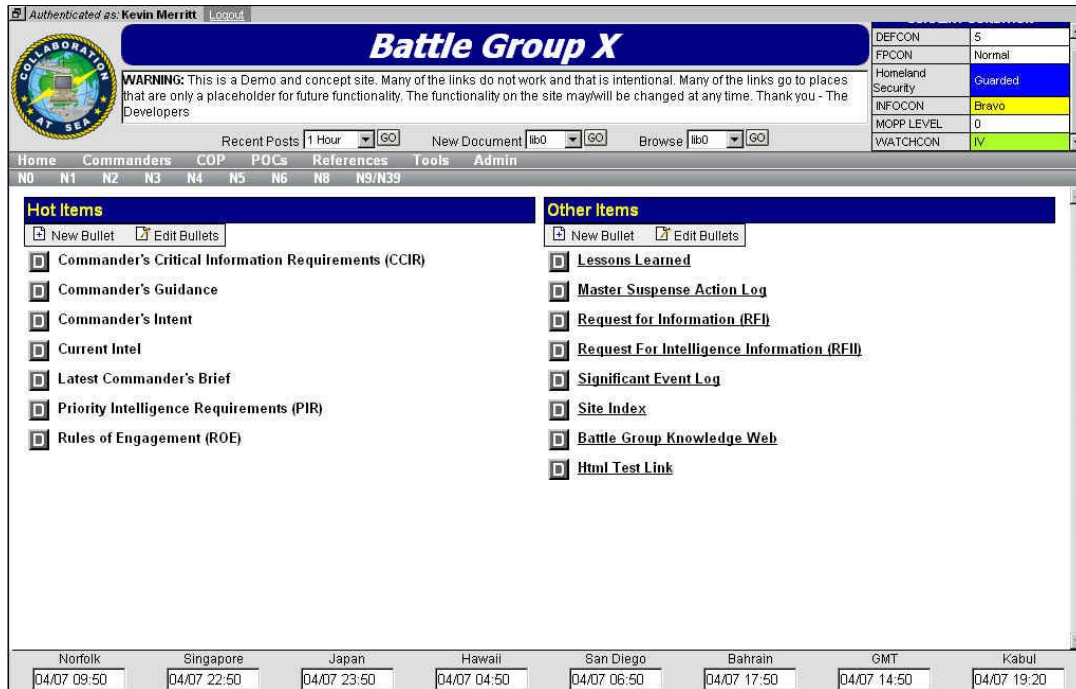




Figure 71 -0 CAS 2.x Front page

- a. Front page images
-  In the top left corner of the site, this icon allows the header and footer to be hidden.
 -  In the top left corner of the site, when the header and footer is hidden, this icon allows the header and footer to be shown.

b. Header

- (a) Header section contains the following items: Command Group image, text box for emergent news, and the navigation tools to reach Recent Posts, New Document, and Browse. Designated administrators from the command will have access to alter the Logo, the emergent news, and activate/deactivate Recent Posts, New Document, and Browse options.



Figure 72 - Header

c. News

- (a) News is a way to quickly pass along emergent information to the users of the site.

WARNING: This is a Demo and concept site. Many of the links do not work and that is intentional. Many of the links go to places that are only a placeholder for future functionality. The functionality on the site may/will be changed at any time. Thank you - The Developers

Figure 73 - News Entry

d. Footer:

- (a) The Footer on the frontpage contains the clocks tool that can be configured with selected locations or additional locations can be added.

Norfolk	Singapore	Japan	Hawaii	San Diego	Bahrain	GMT	Kabul
04/07 10:39	04/07 23:39	04/08 00:39	04/07 05:39	04/07 07:39	04/07 18:39	04/07 15:39	04/07 20:09

Figure 74 - Clocks (footer)

e. Conditions:

- (a) Condition Charts allow for the shipboard administrators to configure the conditions that are pertinent to their command/unit(s).

CURRENT CONDITION	
DEFCON	5
FPCON	Normal
Homeland Security	Guarded
INFOCON	Bravo
MORP LEVEL	0
WATCHCON	IV

Figure 75 - Conditions Chart

f. Menu:

- (a) The menu tool provides the shipboard administrators with a flexible way to manage the navigation of their site.



Figure 76 - Menu(s)

g. Recent Posts:

- (a) With the configurable Recent Posts Dropdown users can easily see what has been posted in the last hour → last 6 months depending on the frequencies selected.



Figure 77 - Recent Posts Dropdown

h. New Document:

- (a) New document dropdown provides one-click access to post documents the library of the users choice. This tool eliminates the users having to access the library before entering new documents.

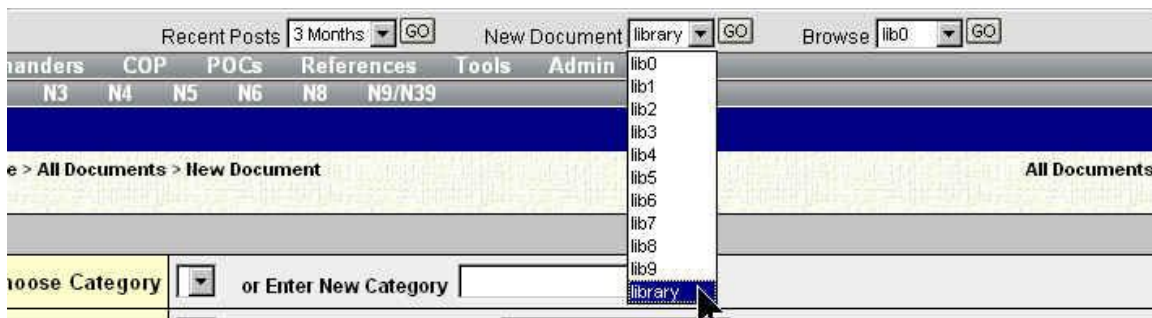


Figure 78 - New Document Dropdown

i. Browse:

- (a) Browse dropdown provides one-click access to the library of the users choice.

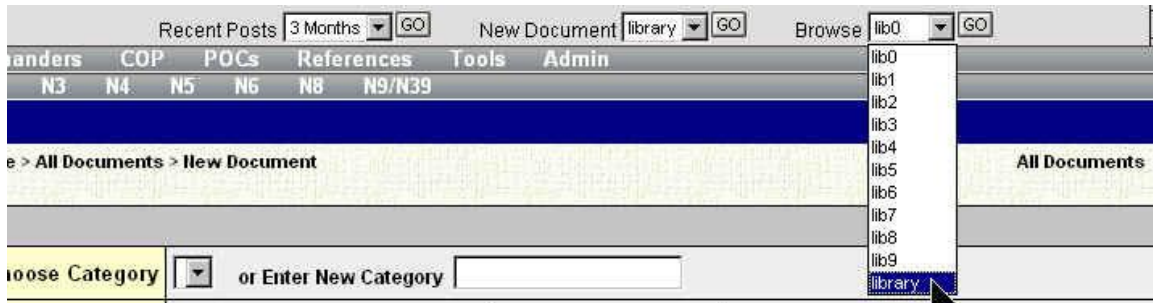


Figure 79 - Browse Dropdown

j. Bullets:

- (a) Links can be added to the front page. Shipboard administrators have the ability to set up the appearance of this page (one/two columns, headings, etc.)



Figure 80 - Front page Links (bullets)

- k. Library Overview
- (a) Configuration Page - Each Document Library comes with its own configuration tool allowing each respective area to set specific features for their library.

You are here: Home > Configuration > Edit Configuration

All Documents | Help | About

Library Settings		
Pre-defined Categories	<div>ATFP; FMO; Chaplain; JAG; MWR</div> <div>Enter a list of pre-defined categories that appears in the drop-down list; separate each entry with a semi-colon.</div>	
Limit entries in Document History	<div>5</div> <div>Enter 0 for unlimited entries.</div>	<input type="checkbox"/> Make Setting Global
Max Size in MB for Documents in Library	<div>0</div> <div>Enter 0 for unlimited size.</div>	<input type="checkbox"/> Make Setting Global
Documents View Default	<div><input checked="" type="radio"/> Expanded By Default <input type="radio"/> Collapsed By Default</div>	<input type="checkbox"/> Make Setting Global
Allow Distribute to All Ships	<div><input checked="" type="radio"/> Hide <input type="radio"/> Allow</div> <div>Note: Will allow users to force documents to all ships in a Battle group</div>	<input type="checkbox"/> Make Setting Global
No. of Columns in Folder View	<div>3</div> <div>Enter number of columns to display in Folder View.</div>	<input type="checkbox"/> Make Setting Global
Content Manager	<div></div> <div>Enter name of point of contact.</div>	
E-Mail Address	<div></div> <div>Enter e-mail address of point of contact.</div>	
Phone Number	<div></div> <div>Enter phone number of point of contact.</div>	
Library Replication Configuration		
Local Temp Dir	<div>C:/Temp/</div>	<input type="checkbox"/> Make Setting Global
Request Library Database	<div>bg2\srrequest.nsf</div>	<input type="checkbox"/> Make Setting Global
Config Document Settings		
Classification	<div>A</div>	
Releasability	<div><input checked="" type="checkbox"/> US <input type="checkbox"/> UK <input type="checkbox"/> AUS <input type="checkbox"/> CAN</div>	
<div><div>Update</div><div>Delete</div><div>Cancel</div></div>		

Figure 81 - Library Configuration

- (b) Shipboard administrators can allow users to be presented with the ability to automatically designate that posted document will be distributed to all of the ships. As shown in Figure 83and **Error! Reference source not found.**, activating this option will add an additional option for file attachments.

Allow Distribute to All Ships	<div><input checked="" type="radio"/> Hide <input type="radio"/> Allow</div> <div>Note: Will allow users to force documents to all ships in a Battle group</div>	<input type="checkbox"/> Make Setting Global
-------------------------------	--	--

Figure 82 - Library Selective Replication – Option

Uncontrolled Copy When Printed

- (c) The user is presented with the distribution options show below in **Error! Reference source not found.** by default. If the site administrators select the Allow option on the Library configuration form (shown in Figure 81 and Figure 82), they use will see the additional option “Distribution to All” as illustrated in Figure 83.

File Attachment	<input type="text"/>	<input type="button" value="Browse..."/>
	<input checked="" type="radio"/> Distribution By Request <input type="radio"/> No Distribution <input type="radio"/> Distribution to All	

Figure 83 - Library Form Upload Field with Option

File Attachment	<input type="text"/>	<input type="button" value="Browse..."/>
	<input checked="" type="radio"/> Distribution By Request <input type="radio"/> No Distribution	

Figure 84 - Library Form Upload Field without Option

LIBRARY DISPLAY PAGE

22. Clicking on the title will take the user to the respective document (attachment, URL, or the text document). If the user is on a low-bandwidth unit, they may be presented with an attachment request form to indicate that they want the document replicated to their unit or a page indicating that the request is in progress.

LIBRARY DISPLAY IMAGES

23. Each of the libraries display images that either show information about the document or provide the user with the ability to access the document information.

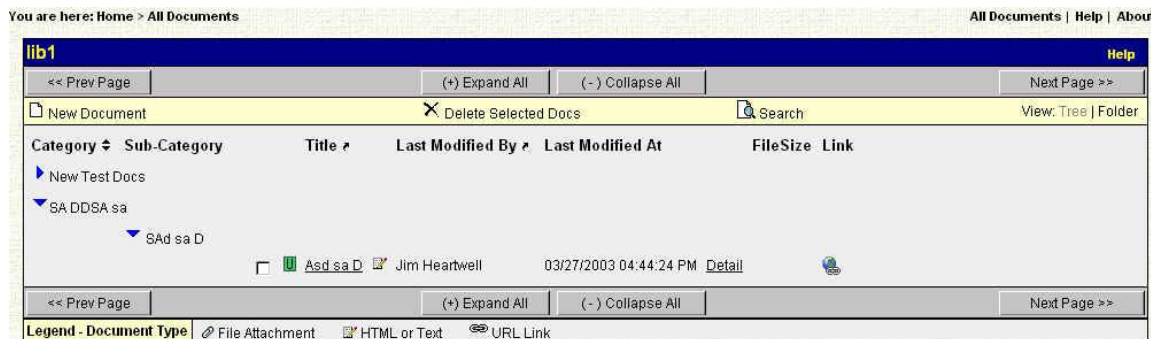
















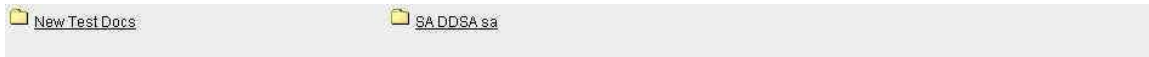
Figure 85 - Library Document Display

	Checkbox that allows user to select more than one document to act upon.				
	Classification Icons to visually display the classification level of the document.				
	Document Type icon to visually indicate the type of document. Options include:				
<table border="1"> <tr> <td>Legend - Document Type</td> <td> File Attachment</td> <td> HTML or Text</td> <td> URL Link</td> </tr> </table>		Legend - Document Type	 File Attachment	 HTML or Text	 URL Link
Legend - Document Type	 File Attachment	 HTML or Text	 URL Link		
	Detail link allows the user to see the form that was completed when document was created.				
	Copy URL icon allows the user to copy the <i>relative</i> URL to the clipboard to be utilized in other applications.				

LIBRARY DISPLAY TREE/FOLDER OPTION

View: Tree | Folder

Clicking on Folder allows the document display to be shown as in the image below (in contrast to the image that appears in 1.14.2):



LIBRARY FORM

You are here: Home > All Documents > New Document All Documents | Configuration | Help | About

Choose Category (R)	ATFP <input type="button" value="v"/> or Enter New Category <input type="text"/>
Choose Sub-Category	<input type="text"/> <input type="button" value="v"/> or Enter New Sub-Category <input type="text"/>
Document Title (R)	<input type="text"/>
Document Description	<input type="text"/>
Open Document in	<input checked="" type="radio"/> Default Frame - Open document in the default window set by the page <input type="radio"/> Current Frame (_self) - Open document in the same window as the current link <input type="radio"/> New Window (_blank) - Open document in a new window <input type="radio"/> Parent Frame (_parent) - Open document in the parent window of the current link
Read-Only	<input type="button" value="v"/> No
Classification	<input type="button" value="v"/> D
Releasability	<input checked="" type="checkbox"/> US <input type="checkbox"/> UK <input type="checkbox"/> AUS <input type="checkbox"/> CAN
Document Type	<input checked="" type="radio"/> File Attachment <input type="radio"/> HTML <input type="radio"/> Text <input type="radio"/> URL Link
File Attachment	<input type="text"/> <input type="button" value="Browse..."/> <input checked="" type="radio"/> Distribution By Request <input type="radio"/> No Distribution
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 86 - Library Form

24. The document in the library allows the user to post document in a category and sub-category (if applicable). Since CAS 2 is supporting selective replication, adding a description of your attachment will help surface combatants and submarines determine if they need to download the attached file. With the title and the description along with the meta data, any users on bandwidth-restricted ships should be able to determine if they want a copy of the file.

25. The editors can also specify if they want to restrict access to the document when it is posted to the library. Editors also will specify the type of document being posted.

Document Type	<input type="radio"/> File Attachment <input checked="" type="radio"/> HTML <input type="radio"/> Text <input type="radio"/> URL Link
HTML	Note: Any HTML greater than 15KB will be automatically converted into a file attachment.
	<div data-bbox="407 569 1313 602"><div>Arial 1 (8 pt) B I U [List Icons] [Text Color Icon] [Background Color Icon] <></div><div></div></div>

Figure 87 - Library Document Type – HTML

26. The rich text field in this application has been improved. Allowing the users to edit the text and add a number of special formatting to the text including HTML.

Document Type	<input type="radio"/> File Attachment <input type="radio"/> HTML <input checked="" type="radio"/> Text <input type="radio"/> URL Link
Text	Note: Any HTML/text greater than 32KB will be automatically converted into a file attachment Preview Document
	<div></div>

Figure 88 - Library Document Type – Text

27. As with prior versions of CAS, users can elect to add text (Figure 88) and a URL link (Figure 89).

Document Type	<input type="radio"/> File Attachment <input type="radio"/> HTML <input type="radio"/> Text <input checked="" type="radio"/> URL Link
URL Link	<div style="border: 1px solid black; height: 30px; width: 100%;"></div> <p>Include http:// if link is absolute. Preview Link</p>

Figure 89 - Library Document Type - URL Link

28. As with all of the CAS links, special care should be taken to ensure that the URLs entered are relative. Using URLs that include the IP address (205.x.x.x) or the DNS entry `http://cas` will cause the link to force users to return to the server where the original document was posted OR fail.

LIBRARY FORM – SELECTIVE REPLICATION REQUEST

29. When an attachment is added to the form user has the ability to indicate if and how this information is shared with others.

File Attachment	<input type="text"/>	<input type="button" value="Browse..."/>
	<input checked="" type="radio"/> Distribution By Request <input type="radio"/> No Distribution	

Figure 90 - Distribution by Request

30. When a document is set to “Distribution by Request,” the user on a low-bandwidth ship will see a File Request Form indicating that the document has not been replicated to the server and they will need to click the request button. The document will be replicated to the ship within 60/90 minutes depending on the size of it and the other documents that need to be replicated.

File Request Form	
File Status	The Attachment you have selected does not exist on your local server. Click on the Request button below to request the attachment during the next replication cycle. It should then be on your server within 60 minutes, network connectivity permitting.
File Requested	ELEPHANT.MPG
File Size	693 KB
Database	bg2\lib0.nsf
UserName	Kevin Merritt
Replicate To Server	137.247.11.90
<input type="button" value="Request"/> <input type="button" value="Cancel"/>	

Figure 91 - Library Selective Replication Request Form

LIBRARY FORM – SELECTIVE REPLICATION STATUS

31. Until the document is replicated to the site, when users click on the document link, they will be presented with a status form, indicating that the document was requested and that the status is “*In Process*”

File Attachment Status Form	
File Status	The Attachment requested is not currently on your local server. It has already been request by the Requestor below, and should be on your local CaS server within a maximum of 60 minutes, network connectivity permitting.
Original Requestor	Kevin Merritt
Request Status	In Process
Replicate To Server	137.247.11.90
<input type="button" value="Cancel"/>	

Figure 92 - Library Selective Replication Status Page

LIBRARY – SELECTIVE REPLICATION PROCESSES

DISTRIBUTION BY REQUEST PROCESS

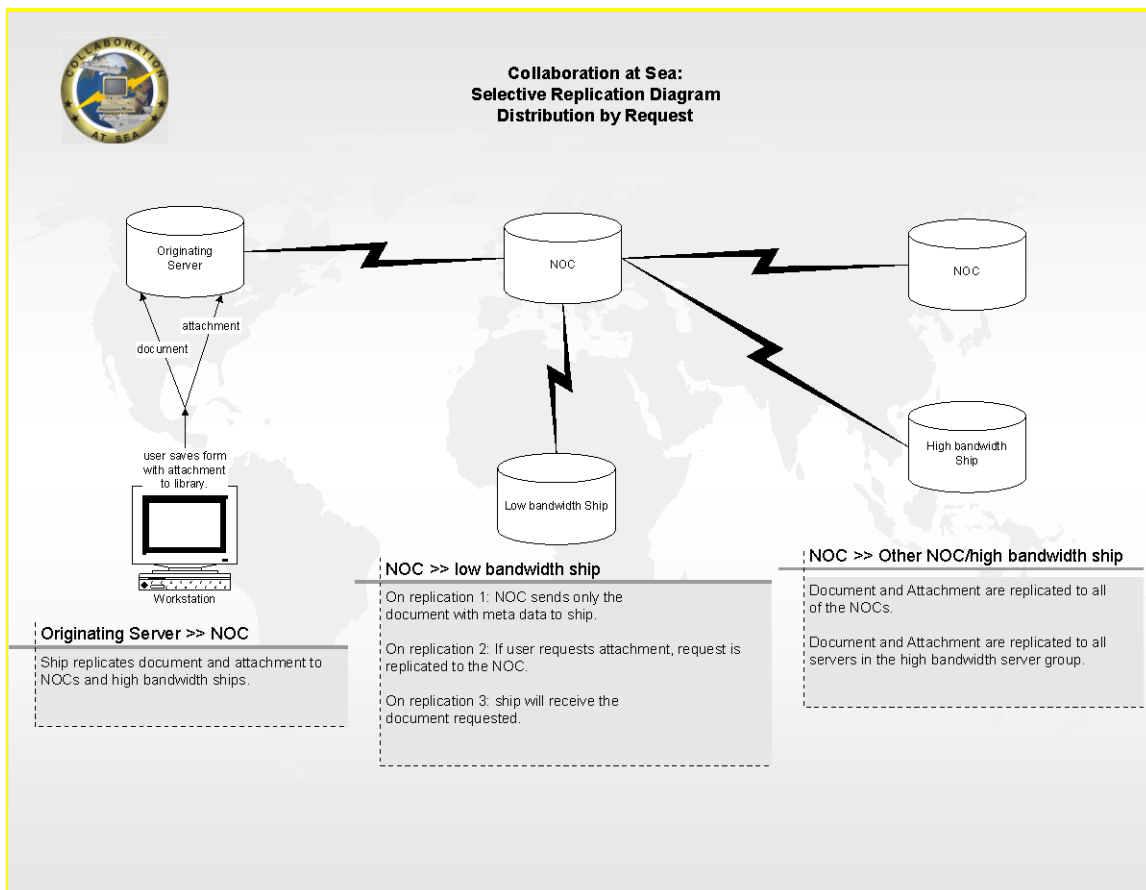
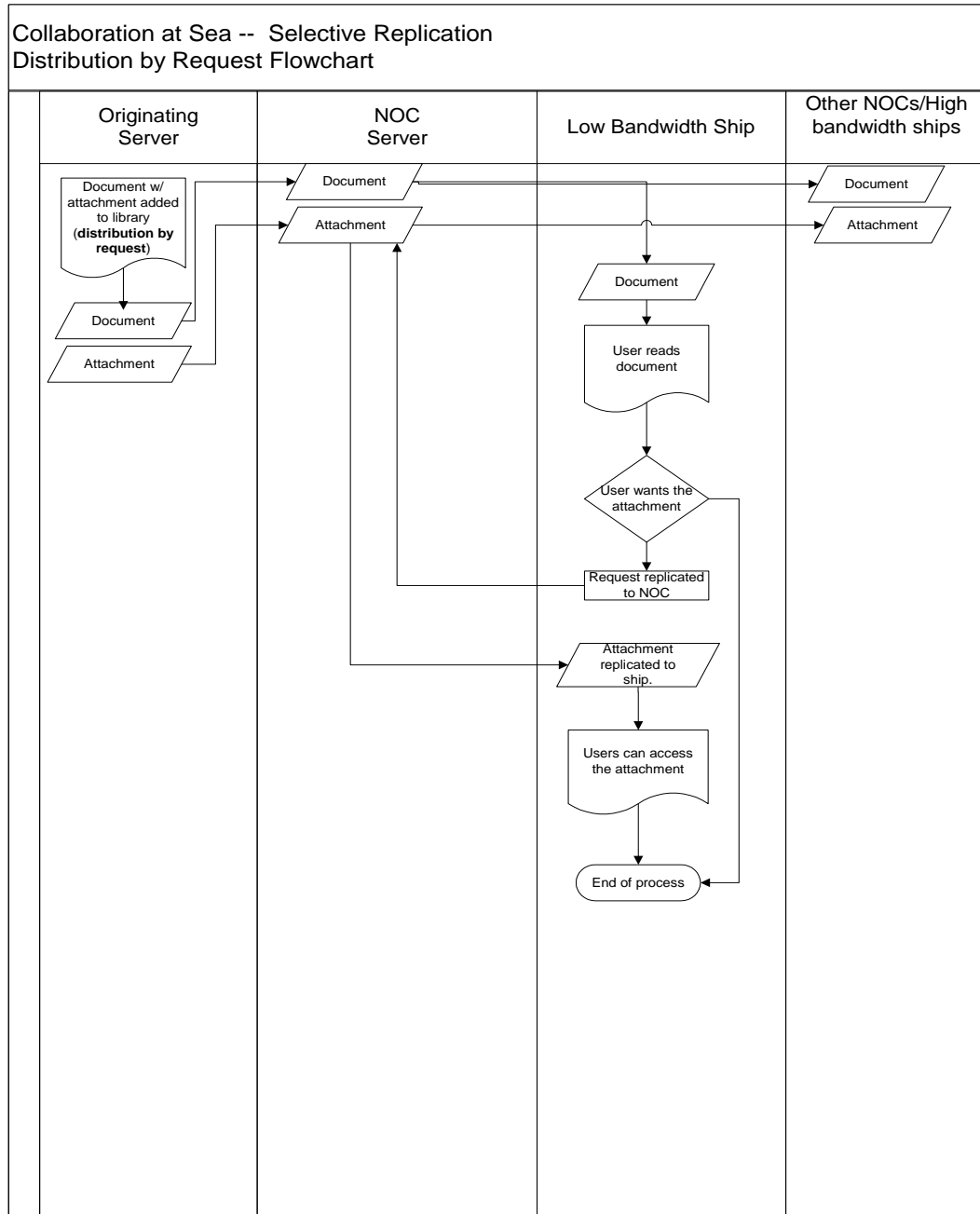


Figure 93 - Selective Replication -Distribution by Request Diagram

DISTRIBUTION BY REQUEST FUNCTIONAL FLOWCHART



Uncontrolled Copy When Printed

Figure 94 - Selective Replication - Distribution by Request Flowchart

NO DISTRIBUTION PROCESS

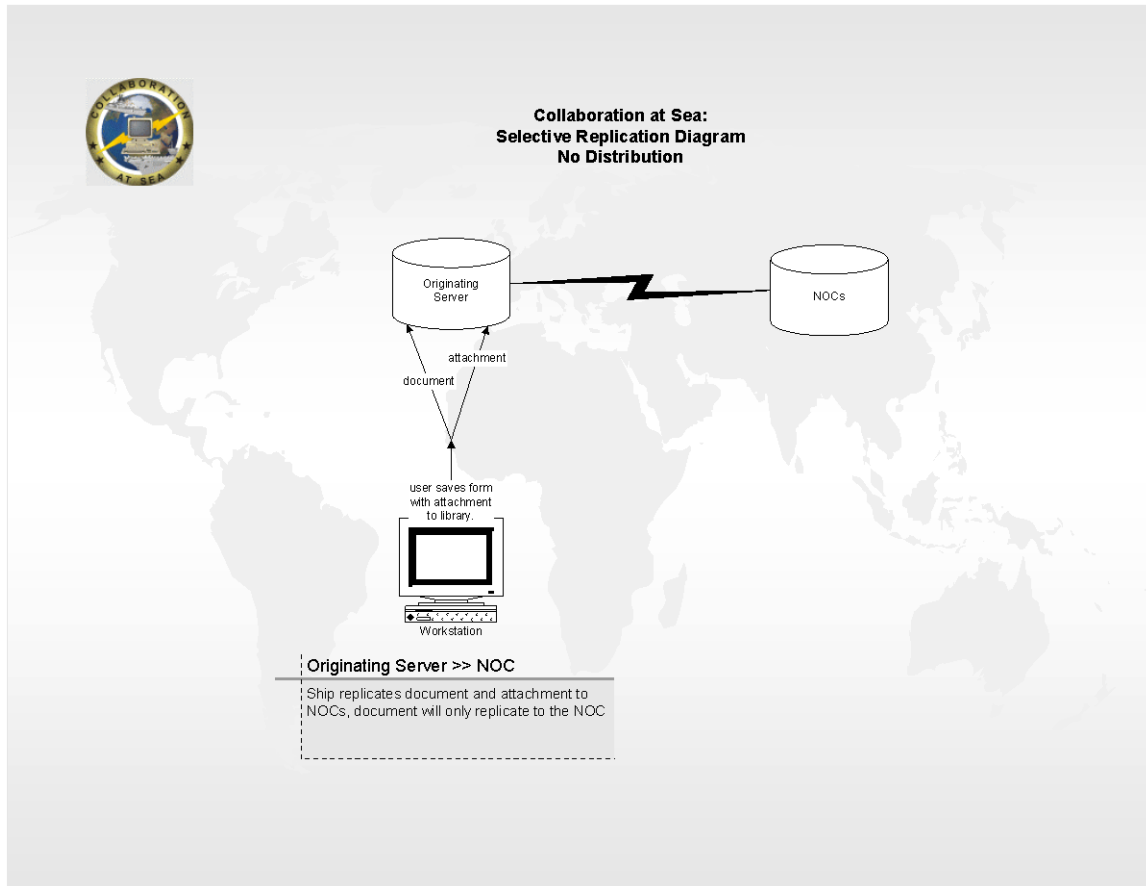


Figure 95 - Selective Replication - Optional Distribute to All Diagram

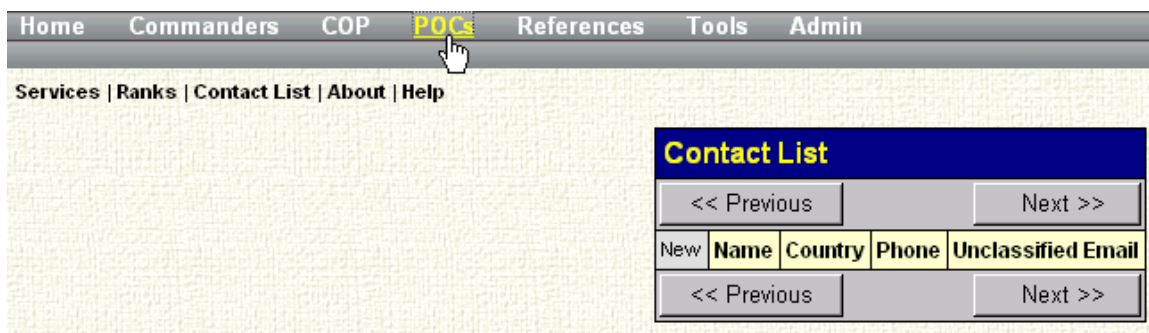
OPTIONAL -- DISTRIBUTE TO ALL PROCESS**POINT OF CONTACT**

Figure 96 - POC Section

SERVICE

Service Listing		
<< Previous		Next >>
New	Country	Service
Edit	AUSTRALIA	RAN
Edit	CANADA	CN
Edit	GREAT BRITAIN	RN
Edit	UNITED STATES	Other
Edit	UNITED STATES	USA
Edit	UNITED STATES	USAF
Edit	UNITED STATES	USCG
Edit	UNITED STATES	USMC
Edit	UNITED STATES	USN
<< Previous		Next >>

Figure 97 - POC Service Listing

Uncontrolled Copy When Printed

RANK

Rank Listing					
<< Previous			Next >>		
New	Country	Service	Rank	Description	Option
Edit	UNITED STATES	USN	PO2	Petty Officer Second Class	None
Edit	UNITED STATES	USN	PO1	Petty Officer First Class	None
Edit	UNITED STATES	USN	CPO	Chief Petty Officer	None
Edit	UNITED STATES	USN	SCPO	Senior Chief Petty Officer	None
Edit	UNITED STATES	USN	MCPO	Master Chief Petty Officer	None
Edit	UNITED STATES	USN	CWO2	Chief Warrant Officer W2	None
Edit	UNITED STATES	USN	CWO3	Chief Warrant Officer W3	None
Edit	UNITED STATES	USN	CWO4	Chief Warrant Officer W4	None
Edit	UNITED STATES	USN	ENS	Ensign	None
Edit	UNITED STATES	USN	LTJG	Lieutenant Junior Grade	SEL
Edit	UNITED STATES	USN	LT	Lieutenant	None
Edit	UNITED STATES	USN	LCDR	Lieutenant Commander	SEL
Edit	UNITED STATES	USN	CDR	Commander	None
Edit	UNITED STATES	USN	CAPT	Captain	SEL
Edit	UNITED STATES	USN	RDML	Rear Admiral Lower Half	SEL
Edit	UNITED STATES	USN	RADM	Rear Admiral Upper Half	SEL
Edit	UNITED STATES	USN	VADM	Vice Admiral	SEL
Edit	UNITED STATES	USN	ADM	Admiral	SEL

Figure 98 - Rank Listing

Uncontrolled Copy When Printed